1/2018

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

41. Jahrgang
ISSN 0137-7767
12,00 Euro



Polizeigesetze – Verschärfungen allerorten

■ Regierungsparteien ohne Vision bei der Digitalisierung ■ Sicherheitsgesetze in Deutschland ■ Neuordnung des Bayerischen Polizeirechts ■ Auswertung von DNA-Daten ■ Entwürfe der neuen Polizeigesetze für Niedersachsen, Nordrhein-Westfalen, Bremen und Hessen ■ Berliner Allianz für Freiheitsrechte gegründet ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Freitag, 25. Mai 2018
Gültigwerden der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)

Mittwoch, 01. August 2018
Redaktionsschluss DANA 3/2018

Sonntag, 09. September 2018
Vorstandssitzung der DVD in Kiel
Interessenten melden sich bitte in der Geschäftsstelle der DVD an.

Montag, 10. September 2018
Sommerakademie des ULD Schleswig-Holstein
https://datenschutzzentrum.de/sommerakademie/2018/

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
41. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Dr. Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
pixelio, Adobestock, ClipDealer

Editorial

Menschen verhalten sich beim Einsatz digitaler Technik oft scheinbar widersprüchlich, nicht rational. Dies wird oft mit dem Begriff Privacy Paradox beschrieben. Es sind nicht objektive Interessen und explizite Wünsche und Notwendigkeiten, die unser digitales Leben lenken, sondern oft versteckte unbewusste Wünsche und deren Ausbeutung durch Geschäftemacher und politische Manipulatoren. Das Whistleblowing über Cambridge Analytica und Facebook hat diesen Umstand und den Datenschutz wieder in die Schlagzeilen gebracht. So paradox manches erscheinen mag, so logisch ist es bei einer analytischen ökonomischen, politischen oder psychologischen Betrachtung.

Ein solches Paradox wurde kurzfristig das Schwerpunkthema dieses Heftes: Weshalb beschließt die Politik immer wieder offensichtlich verfassungswidrige Sicherheitsgesetze, wohl wissend, dass diese später von Gerichten wieder aufgehoben werden. Auch hier muss in sozialen Wissenschaften, der Psychologie und Politologie gegraben werden, um definitiv fündig zu werden:

Politiker suchen wie Internet-User nach Belohnung und Ich-Bestärkung. Diese gewinnt man nicht unbedingt durch stille und demütige Förderung des Gemeinwohls, sondern eher durch Übermaß und Skandalisierung. Wie kleine Kinder versuchen zumindest manche Politiker (es sind kaum Frauen) ihre Grenzen der Macht auszutesten, indem sie – unter Applaus einer populismusanfälligen Öffentlichkeit – Law and Order nicht nur predigen, sondern auch praktizieren. Ein eklatantes Beispiel liefert uns derzeit die bayerische Politik und zugleich ein weiteres Paradoxon: Obwohl es das Gemeinwohl nachhaltig durch Rundumüberwachung zu schädigen droht, wird das geplante bayerische Polizeirecht fast nicht zur Kenntnis genommen. Entsprechendes gilt für weitere Sicherheitsgesetze. Das vorliegende Heft will dieser Unkenntnis bzw. Nichtkenntnisnahme ein wenig abhelfen.

Thilo Weichert, DVD-Vorstandsmitglied



Bild: ClipDealer

Autorinnen und Autoren dieser Ausgabe:

Freiheitsfoo,
https://freiheitsfoo.de/

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Presseerklärung vom 07.02.2018

DVD: „Regierungsparteien ohne Vision bei der Digitalisierung"



Bild: AdobeStock

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) findet im Koalitionsvertrag von CDU/CSU und SPD keine Impulse für eine freiheitliche und demokratische Gestaltung des Einsatzes von Informationstechnik. Zwar wirbt die Union mit „Lust auf Digitalisierung". Die SPD spricht vom „Zukunftsentwurf". Tatsächlich steht die Häufigkeit des Begriffs „Digitalisierung" im geplanten schwarz-roten Vertrag im umgekehrten Verhältnis zu konstruktiven Vorschlägen zur Bewältigung der damit verbundenen gesellschaftlichen Risiken. Der Ausbau des Glasfasernetzes und der Aufbau von 5G-Mobilfunk stehen auf der Tagesordnung, eGovernment und Förderung der Digitalisierung in allen Lebensbereichen, das war es dann auch. Die Beschlüsse von Schwarz-Rot zur Digitalisierung folgen praktisch durchgängig dem Prinzip des Vorrangs der Wirtschaft vor den Bürgerinnen und Bürgern. Selbst der juristische Unsinn eines „Dateneigentums" findet sich im Text. Die Weiterentwicklung des Datenschutzes, die Produkthaftung von IT-Produktanbietern, Sammelklagemöglichkeiten bei Verbraucher- oder Datenschutzverstößen, spezifische Algorithmenkontrollen, Open Access und mehr Informationsfreiheit, digitalisierungsorientierte Steuermodelle, Flexibilisierungsschutz für Beschäftigte – alles Fehlanzeige. Zum Beschäftigtendatenschutzgesetz wurde ein folgenloser Prüfauftrag formuliert. Eine digitale Grundrechte-Charta wird immerhin erwähnt.

DVD-Vorsitzender Frank Spaeing: „Freiheitliche, demokratische und bürgerorientierte Digitalisierung geht anders. Die CSU stellt den Digitalminister und macht damit wieder den Bock zum Gärtner." Werner Hülsmann, stellvertretender DVD-Vorsitzender: „Die Fehlanzeigen bei der Gestaltung der Digitalisierung müssen nicht bedeuten, dass diese in den nächsten vier Jahren ausgeschlossen ist. Nötig ist dafür eine öffentliche Debatte, eine außerparlamentarische Bürgerbewegung, die Druck macht – für eine freiheitliche, demokratische und soziale Digitalisierung. Die DVD wird dazu gerne ihren Beitrag leisten."

Thilo Weichert

Sicherheitsgesetze in Deutschland – vom Aus- und Überreizen des verfassungsrechtlich noch Akzeptablen –

„Alle schauen auf das brennende Haus – nur Klaus schaut raus". So ließe sich kurz die aktuelle Situation der durch Klaus personifizierten Bürgerrechte in der deutschen Sicherheitspolitik beschreiben. Ob die Hoffnung auf die Feuerwehr, durch das Bundesverfassungsgericht und den Europäischen Gerichtshof personifiziert, gerechtfertigt ist, muss sich mal wieder erweisen. Brandstifter ist diesmal vor allem die Bayerische Staatsregierung, an deren Spitze zum Einbringen der Novellierung des Polizeiaufgabengesetzes (PAG)[1] noch Horst Seehofer vorstand. Dieser ist inzwischen Innenminister auf Bundesebene und damit dort für die Polizeigesetzgebung zuständig. Aber er ist nicht das personifizierte „Böse". Entsprechende Pläne werden auch in anderen Bundesländern und durch andere Politiker verfolgt.

1 Das Ping-Pong der Sicherheitsgesetzgebung

Das deutsche Sicherheitsrecht zeichnet sich durch eine Art Ping-Pong aus, das schon seit langem, insbesondere wieder seit dem Jahr 2004 „gespielt" wird, als das BVerfG mit einem großen Paukenschlag den großen Lauschangriff bremste[2]: Es werden grundrechtsverletzende Normen beschlossen, die höchstrichterlich aufgehoben werden müssen. Darauf erfolgt eine normative Anpassung. Dies hindert aber Exekutive und Legislative nicht, wiederum – zumeist andere – grundrechtsverletzende Normen zu beschließen, die wieder aufgehoben werden. Nach dem Anschlag des 11. September 2001 stellte das höchste deutsche Gericht mit seiner Entscheidung zum Lauschangriff klar, dass es nicht bereit ist, in die Populismusfalle der Terrorbekämpfungshysterie einzustimmen, dass es gewillt ist, unsere Grundrechte stimmungsunabhängig zu verteidigen. Seit der Begründung des Grundrechts auf informationelle Selbstbestimmung mit dem Volkszählungsurteil Ende 1983[3] verfolgt damit das BVerfG einen grundrechtsfreundlichen rechtsstaatlichen Kurs bei informationellen Eingriffen. Die Legislative wie auch die Exekutive müssen regelmäßig daran erinnert werden, dass wir in einem Rechtsstaat leben, bei dem Sicherheitsbedürfnisse nicht über alles gestellt, sondern abgewogen werden müssen.

Seit 2009 haben wir in der Europäischen Union (EU) eine Grundrechte-Charta (GRCh), in der Grundrechtsstandards, wie wir sie für Deutschland aus dem Grundgesetz (GG) kennen, und wie sie nominell auch in der Europäischen Menschenrechtskonvention (EMRK) verbrieft sind, EU-weit normativ und mit einem effektiven Rechtsschutzverfahren etabliert werden. Eine gewisse Zeit war nicht klar, inwieweit der zur Kontrolle der GRCh vorgesehene Europäische Gerichtshof (EuGH) seine Funktion als Hüter der Grundrechte auch gegenüber der Legislative und der Exekutive auf höchster Ebene wahrnehmen würde. Diese Unsicherheit wurde insbesondere durch zwei Entscheidungen genommen: die Aufhebung der Richtlinie zur Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten April 2014[4] und des Safe-Harbor-Rechtsrahmens der EU-Kommission zur Datenübermittlung in die USA im Oktober 2015.[5] Dass der EuGH auch vor mächtigen Privatfirmen Gleichheit im Recht und Grundrechtsschutz zu wahren gewillt ist, zeigte er im Mai 2014 gegenüber Google.[6]

Also: Alles gut? Leider nein. Das Ping-Pong hat kein Ende. Dafür gibt es Gründe: Die technische Entwicklung eröffnet immer wieder neue Möglichkeiten sicherheitsbehördlicher Eingriffe in informationelle Grundrechte, bei denen noch nicht explizit höchstrichterlich festgestellt wurde, dass diese nicht bzw. unter welchen Voraussetzungen diese zugelassen werden dürfen. Ein weiterer Grund ist, dass die Populismusbereitschaft etablierter Parteien durch die nicht nur vorübergehende Präsenz der AfD auf der politischen Bühne befördert wurde. Daneben gibt es einen strukturell angelegten Grund, weshalb das Ping-Pong-Spiel kein Ende finden wird: Gesetze werden von der Exekutive vorbereitet, die ein professionelles Interesse daran hat, ihre Befugnisse auszuweiten. Die Lernbereitschaft der Exekutive, nicht nur zugunsten der eigenen Aufgabenerfüllung (als eine Form der Selbstbestätigung und Daseinsrechtfertigung), sondern zugunsten eines übergeordneten Gemeinwohls tätig zu werden, zu dem auch demokratische Transparenz und der Schutz der Freiheitsrechte gehören, muss immer wieder erneuert werden.

2 Aktuelle Sicherheitsgesetze und Vorhaben hierfür

Derzeit macht es wieder „Ping": Von der Öffentlichkeit bisher weitgehend unbeobachtet wird das Recht der Sicherheitsbehörden auf Bundes- wie auf Länderebene gerade massiv erneuert. Anlass ist einmal mehr die Vorgabe des BVerfGs, durch die ein umfassendes Polizeigesetz, das Gesetz zum Bundeskriminalamt (BKA-G) aus dem Jahr 2008,[7] einer umfassenden verfassungsrechtlichen Korrektur unterworfen wurde. Die Bewertung des BVerfG wies auf teilweise kleine, teilweise aber auch gravierende Nachbesserungsnotwendigkeiten hin. Mensch hätte nun den Eindruck haben können, dass in diesem Urteil, das in sage und schreibe 359 Randnummern gegliedert ist und mit zwei abweichen-

den Meinungen, die weitere 45 Randnummern füllen, alles Wesentliche zum Verhältnis von Sicherheit und Freiheit gesagt wäre.

Aber weit gefehlt: Die ersten gesetzgeberischen Reaktionen orientierten sich 2017 noch weitgehend an den verfassungsrechtlichen Vorgaben, nämlich beim BPolG, bei dem mobile Bild- und Tonaufzeichnungsgeräte (vulgo Bodycams) und anlassbezogene Kfz-Kennzeichen-Erfassung geregelt wurde[8], und bei der vollständigen Überarbeitung des BKA-G[9].

Doch auch das Bundesland Bayern überarbeitet sein Sicherheitsrecht. Es hatte mit einer ersten Novelle des PAG vom 24.07.2017 schon einmal Duftmarken gesetzt, als es den bis dahin im deutschen Polizeirecht nicht existierenden Rechtsbegriff der „drohenden Gefahr" eingeführt hat.[10]

In Baden-Württemberg wurde Ende 2017 ein Polizeigesetz verabschiedet, in dem die präventive Telekommunikationsüberwachung (TKÜ) einschließlich Quellen-TKÜ zur Abwehr von dringenden Gefahren schwerwiegender Rechtsgüter sowie die sog. „intelligente Videoüberwachung" an „gefährdeten Objekten", Kriminalitätsschwerpunkten und bei „öffentlichen Veranstaltungen und Versammlungen, wenn dort terroristische Anschläge drohen" erlaubt werden. Nach Bayern erlaubt Baden-Württemberg als zweites Bundesland „Aufenthaltsvorgaben, Kontaktverbote sowie die Überwachung durch elektronische Fußfesseln" zur Verhütung von Straftaten nach § 129a StGB.[11]

In Hessen[12], Niedersachsen[13], Nordrhein-Westfalen[14] und Bremen[15] befinden sich weitere Polizeigesetzänderungen in der Mache.

Auch das Recht der Geheimdienste wurde auf Bundesebene durch Änderungen des BVerfSchG in den Jahren 2015[16], 2016[17] und 2017[18] sowie des BND-G im Jahr 2016[19] umfassend überarbeitet. Auf Länderebene wurden die Verfassungsschutzgesetze von Nordrhein-Westfalen bis 2018 mehrfach[20] sowie von Thüringen 2015[21], Bayern[22] und Niedersachsen[23] im Jahr 2016 sowie Baden-Württemberg[24] im Jahr 2017 erneuert. In Hessen wird ein äußerst umstrittener Entwurf diskutiert.[25]

Im Bereich der Strafverfolgung ist ebenso kein Ende der Gesetzgebung erkennbar. Im Jahr 2015 wurde die sog. Vorratsdatenspeicherung von Telekommunikationsdaten erneut geregelt,[26] nachdem ein Vorgängergesetz vom BVerfG kassiert worden war.[27] Zwar hat das BVerfG in Eilentscheidungen die aktuellen Regelungen für vorläufig anwendbar erklärt,[28] doch hat es schon nach einer entsprechend kritischen Entscheidung des EuGH[29] signalisiert, dass im Hauptsacheverfahren erneut Korrekturen gefordert werden müssten.[30] Die vorläufig letzte Regulierung der Strafprozessordnung (StPO) erfolgt mit dem „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens", bei dem u. a. Ausweitungen der Befugnisse zur DNA-Analyse sowie zur Einführung der sog. „Online-Durchsuchung" vorgesehen wurden.[31]

3 Schwarz-Weiß-Diskussionen

Die Auseinandersetzung um die Vorratsspeicherung von Telekommunikationsverkehrsdaten ist ein fast typischer Fall für die Art der Auseinandersetzung zu Befugnissen im Sicherheitsbereich. Diese Auseinandersetzung dauert schon mehr als 20 Jahre. 1996 forderte der Bundesrat erstmals die Einführung von „Mindestfristen" für die Speicherung von Verbindungsdaten.[32] Nachdem im Bundesinnenministerium festgestellt worden war, dass auf nationaler Ebene diese Forderung kurzfristig nicht umgesetzt werden könnte, wurde auf europäischer Ebene eine entsprechende Richtlinie angeschoben, die 2006 tatsächlich erlassen wurde. Die öffentliche Diskussion drehte sich von Anfang an um die Grundsatzfrage, ob überhaupt eine Verpflichtung zu einer vorsorglichen Speicherung von TK-Verkehrsdaten erlaubt werden soll – ja oder nein.

Bei dieser Diskussion spielten die konkreten und differenzierten sicherheitsbehördlichen Bedarfe sowie Vorschläge zur Begrenzung der Maßnahme erst eine Rolle, nachdem dies von der höchstrichterlichen Rechtsprechung eingefordert wurde. Selbst beim Aushandeln der aktuell geltenden Regelung zwischen SPD und CDU/CSU als Regierungsparteien ging es bis zum Ende um Grundsatzpositionen, während die schon sehr präzisen Vorgaben des BVerfG zu den jeweiligen Zwecken, der Speicherdauer, der Art der Daten sowie den prozeduralen Anforderungen weiterhin nur eine nachgeordnete Rolle spielten.

Diese in großem Maße irrationale Debatte wiederholt sich bei vielen weiteren sicherheitsbehördlichen Befugnissen: Die Gesetzesvorschläge starten zunächst mit Maximalforderungen und ohne Netz und doppelten Boden. Der aktuelle bayerische PAG-Entwurf ist hierfür ein beredtes Beispiel: Da wird rechtlich die digitale „Durchsuchung" mit der Durchsuchung von körperlichen Sachen gleichgesetzt, obwohl das Vorgehen, die Eingriffstiefe, die damit verbundenen Risiken wie auch die nötigen grundrechtssichernden Maßnahmen sich grundsätzlich von körperlichen Durchsuchungen unterscheiden. Diese Vorgehensweise beruht bei der Politik vielleicht auch auf fehlender Kenntnis der fachspezifischen Gegebenheiten und Bedingungen. Bei den diese Maßnahme einfordernden Behördenvertretern, die der Politik die Vorschläge unterbreiten, müssten aber diese Detailkenntnisse vorliegen. Wäre dies nicht der Fall, so wäre dies geradezu kriminell; fehlt Sicherheitsbehörden das Risikobewusstsein für ihr eigenes Tun, dann steht es schlecht um die Sicherheit.

Weitere Beispiele aus dem bayerischen PAG-Entwurf sind der Einsatz von Drohnen, die Nutzung von Mustererkennung sowie die Durchführung genetischer Phänotypisierung. Derartige Maßnahmen finden sich auch schon teilweise in anderen Sicherheitsgesetzen. Doch in der Undifferenziertheit und Unverfrorenheit, wie sie in Bayern geregelt werden sollen, bleibt dieses Bundesland einzigartig.

Der weitere Ablauf ist absehbar: Die Gerichte werden Bedenken äußern, Maßnahmen nur einschränkend zulassen oder gar vollständig verbieten. Dann wird wieder nachgebessert werden müssen. Bis dann die Regulierung einigermaßen demokratie- und grundrechtsverträglich ist, kann es wieder Jahre, vielleicht viele Jahre dauern, in denen nicht nur Rechtsunsicherheit herrscht, während denen vielmehr Grundrechte in der Praxis missachtet werden. Dies



Bild: Frans Valenta

ist kein schönes Spiel. Auch wenn es wie ein Spiel scheint: Dies ist Ernst und bringt reale Opfer zutage.

4 Die Positionen der Parteien

Bei der Auseinandersetzung um sicherheitsbehördliche informationelle Befugnisse sind natürlich die programmatischen Positionen der in den Parlamenten vertretenen politischen Parteien von Bedeutung. Während die CDU/CSU regelmäßig und manchmal schon ermüdend gebetsmühlenhaft für eine Ausweitung der Befugnisse eintritt, äußern sich Die Linken, Bündnis 90/Die Grünen und die FDP eher skeptisch bis ablehnend. Bei der SPD kommt es darauf an, inwieweit sie sich durch ihre Position in der Opposition gegenüber einer Regierungspolitik profilieren kann; als Regierungspartei hat sie sich aber regelmäßig mit der CDU/CSU auf „Kompromisse" eingelassen, die später einer verfassungsrechtlichen Überprüfung nicht standgehalten haben.

Dieser Unterschied ist auch bei den anderen Parteien feststellbar. Bei der FDP ist dies besonders eklatant. Sie versucht sich in der Opposition grundsätzlich als Bürgerrechtspartei zu profilieren; als Regierungspartei akzeptiert sie dagegen weitgehend exekutive Forderungen. Diese Aussage gilt für den wirtschaftsliberalen Flügel der Partei uneingeschränkt; ein kleiner aber wortstarker Bürgerrechtsflügel profiliert sich bürgerrechtlich auch innerhalb von Regierungen. Am eindrucksvollsten war insofern der Rücktritt der damaligen FDP-Justizministerin Sabine Leutheusser-Schnarrenberger am 14.12.1995, nachdem ihre Partei beschlossen hatte, der Gesetzesinitiative zum später vom BVerfG kassierten großen Lauschangriff zuzustimmen. Leutheusser-Schnarrenberger sowie weitere verdiente FDP-Innen- und Justizpolitiker, insbesondere Burkhard Hirsch und Gerhard Baum, traten dann auch oft als Kläger gegen Sicherheitsgesetze von dem BVerfG auf. Diese Bürgerrechtsprotagonisten werden von ihrer Partei gerne zu Wahlkampfzeiten präsentiert. Hat die FDP Regierungsverantwortung, so werden ihre Bedenken eher ignoriert, so wie sich dies derzeit in Nordrhein-Westfalen bzgl. der geplanten Polizeirechtsänderung wieder abzeichnet. Der Wirtschaftsflügel, der mit „Digitalisierung first, Bedenken second" im Herbst 2017 Bundestagswahlkampf machte, hat – trotz der Oppositionsrolle und eines weit verbreiteten Relevanzverlustes der FDP – derzeit offensichtlich die Oberhand. Die undifferenzierte Digitalisierungseuphorie macht auch vor dem sicherheitsbehördlichen Einsatz nicht halt.

Ähnliche Prozesse lassen sich bei Bündnis 90/die Grünen feststellen. Auch dort gibt es eine kleine Gruppe von engagierten Bürgerrechtlern. Für diese Gruppe stehen z. B. Christian Ströbele, Jan-Philipp Albrecht oder Konstantin von Notz. Trotz ihrer bürgerrechtlichen Wurzeln und geäußerter Bedenken konnten die Grünen nach den Anschlägen am 11.09.2001 die teilweise offensichtlich unverhält-

nismäßigen Sicherheitspakete des damaligen SPD-Bundesinnenministers Otto Schily nicht verhindern. Für die Mehrheit von Bündnis 90/die Grünen stehen digitale Bürgerrechte heute mehr nicht im Vordergrund. Den Nachweis hierfür liefern sie in den Koalitionen mit der CDU in Baden-Württemberg und in Hessen.

5 Der Koalitionsvertrag auf Bundesebene

Der Koalitionsvertrag von CDU, CSU und SPD auf Bundesebene macht Vorgaben für die nächsten vier Jahre, weshalb es sinnvoll ist, sich diesen genauer anzuschauen: Schon die Präambel geht auf die Sicherheit in Deutschland ein: „Bürgerinnen und Bürger haben ein starkes Bedürfnis nach ... Sicherheit im Alltag." „Wir wollen, dass die Menschen bei uns ... in Sicherheit leben können." „Wir arbeiten für ... Sicherheit ... in unserem Land." „Gemeinsam ... wollen wir unser Land ... sicherer ... machen".

Im Folgenden sollen den relevanten Aussagen zur „Inneren Sicherheit" des Koalitionsvertrages in ihrer Gänze zitiert werden (Ziffern geben Zeile des Absatzbeginns an):

Pakt für den Rechtsstaat

(5768) Wir werden den Rechtsstaat handlungsfähig erhalten. Dies stärkt auch das Vertrauen in die rechtsstaatliche Demokratie. Wir werden einen Pakt für den Rechtsstaat auf Ebene der Regierungschefinnen und -chefs von Bund und Ländern schließen.

Sicherheitsbehörden

(5786) Bund und Länder haben die personelle Ausstattung der Sicherheitsbehörden bereits vorangebracht. Am Ende dieser Ausbauphase werden insgesamt 15000 Stellen geschaffen worden sein. Der Bund wird 7500 zusätzliche Stellen schaffen. Wir wollen das Bundeskriminalamt als zentrales Datenhaus im polizeilichen Informationsverbund etablieren und einen gemeinsamen Investitionsfonds für die IT der deutschen Polizei schaffen. Im Bereich der Strafverfolgung werden wir den Datenaustausch zwischen Polizei und Justiz verbessern.

Verfahrensrecht

(5795) Wir stärken das Vertrauen in den Rechtsstaat, indem wir die Strafprozessordnung (StPO) modernisieren und Strafverfahren beschleunigen.

(5805) Die DNA-Analyse wird im Strafverfahren auf äußerliche Merkmale (Haar, Augen, Hautfarbe) sowie Alter ausgeweitet (§ 81e StPO).

(5898) Keine Toleranz bei Wirtschaftskriminalität, Einbruchdiebstahl und organisierter Kriminalität. Wir bekämpfen konsequent jede Form von Kriminalität, insbesondere die organisierte Kriminalität. Wohnungseinbrüche führen nicht nur zu materiellen Schäden, sondern häufig zu einer Traumatisierung der Opfer. Unseren Kampf gegen Einbrecher intensivieren wir deshalb weiter, indem wir unseren Sicherheitsbehörden die notwendigen Ermittlungsinstrumente zur Verfügung stellen und die in der vergangenen Legislaturperiode beschlossenen Maßnahmen zur Ahndung und Bekämpfung von Einbruchskriminalität konsequent anwenden.

Sicherheitsarchitektur / Operative Fähigkeiten

(5952) Wir wollen keine Zonen unterschiedlicher Sicherheit in Deutschland. Dazu gehört die Erarbeitung eines gemeinsamen Musterpolizeigesetzes (gemäß Innenministerkonferenz-Beschluss).

(5956) Wir werden uns dafür einsetzen, dass die Bundespolizei bundesweit im Rahmen der bestehenden Zuständigkeiten und Aufgaben eingesetzt wird, so auch zur Bekämpfung von Straftaten an Kriminalitätsschwerpunkten wie z. B. Bahnhöfen, insbesondere von Alltagskriminalität. Die Bereitschaftspolizeien der Länder sowie des Bundes sind eine tragende Säule der inneren Sicherheit und sehen sich einer erhöhten Einsatzbelastung flächendeckend ausgesetzt. Die erforderliche Verbesserung der Ausstattung wird intensiviert.

(5964) Die Menschen sollen sich auf unseren Straßen und Plätzen sicher bewegen können. Deshalb wollen wir die Videoüberwachung an Brennpunkten einsetzen, sie verhältnismäßig und mit Augenmaß effektiv ausbauen und dabei auch technisch verbessern. Intelligente Videoüberwachung kann dabei eine Weiterentwicklung sein. Deswegen werden wir den laufenden Modellversuch abwarten, prüfen und bewerten.

(5975) Bei der Bekämpfung des Terrorismus wollen wir im Rahmen eines zeitgemäßen und effektiven Rechts gemeinsame Standards, verbindlichen Umgang, einheitliche Praxis und klare Zuständigkeitsregelungen. Die Standorte der Bundessicherheitsbehörden sollen bestehen bleiben. Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) werden wir gemeinsam mit den Ländern als Kooperations- und Kommunikationsplattform so weiterentwickeln, dass dort Informationen reibungsloser ausgetauscht und verbindliche Absprachen auch zur Bearbeitung des Einzelfalls getroffen werden.

(5983) Zur Verbesserung der Sicherheit in unserem Land wird das Bundesamt für Verfassungsschutz (BfV) im Bereich der zentralen Auswertung und Analyse in Angelegenheiten des islamistischen Terrorismus sowie bei länderübergreifenden extremistischen Phänomenen von bundesweiter Bedeutung seine Steuerungsfunktion verstärkt wahrnehmen, auch bei solchen, die zunächst keinen unmittelbaren Gewaltbezug aufweisen. Aufgrund des ständigen technischen Fortschrittes und des damit einhergehenden personellen und finanziellen Ressourceneinsatzes soll das BfV als zentrale Servicedienststelle für den Einsatz operativer Technik im Verbund gestärkt werden. Zudem wollen wir die Befugnisse des Verfassungsschutzes des Bundes und der Länder vereinheitlichen, insbesondere bei der Datenerhebung und Datenspeicherung. Zu diesem Zwecke werden wir das Bundesverfassungsschutzgesetz auf Grundlage eines einheitlichen Rechtsrahmens der Innenministerkonferenz novellieren. Wir sind uns bewusst, dass auch maßvolle und sachgerechte Kompetenzerweiterungen des BfV eine gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle erfordern.

(5999) Wir haben in der vergangenen Wahlperiode die gesetzliche Grundlage für eine effektivere Kontrolle der Nachrichtendienste geschaffen. Die Bundesregierung wird diese Kontrolle durch eine umfassende Wahrnehmung der Unterrichtungs- und Vorlagepflichten gegenüber den gesetzlich vorgesehenen Kontrollorganen unterstützen.

(6004) Wir werden die europäische Sicherheitskooperation unter Einbeziehung und Stärkung internationaler und europäischer Organisationen (Europol, Interpol, Europäische Staatsanwaltschaft)

verbessern und vertiefen. Ziel muss es sein, durch strukturelle Maßnahmen und mit einer leistungsfähigen IT-Struktur sicherzustellen, dass Straftäterinnen und Straftäter sowie Gefährderinnen und Gefährder überall in Europa identifiziert und relevante Erkenntnisse ausgetauscht werden können. Zu diesem Zwecke werden wir auf eine effektive Vernetzung und Verbesserung der für die Sicherheitsbehörden relevanten Datenbanken hinwirken. Den Informationsaustausch und die Koordinierung von präventiven und operativen Maßnahmen zwischen den EU-Mitgliedstaaten bei Europol im Rahmen des „European Counter Terrorism Center" und auch die internationale Zusammenarbeit, u. a. im Rahmen von Interpol, wollen wir intensivieren und verbessern. Wir wollen dabei in Absprache mit den Ländern auch die europäische und internationale Zusammenarbeit bei der Bekämpfung der organisierten Kriminalität intensivieren und ebenso die Bekämpfung der Organisierten Kriminalität beim Bundeskriminalamt stärken, um etwa organisierten Einbrecherbanden noch besser zu begegnen.

(6021) Wir bekennen uns zum deutschen Engagement in internationalen Polizeimissionen. Wir werden Möglichkeiten finden, dies auszubauen, etwa durch Einrichtung eines Stellenpools für Auslandsverwendungen und Polizeimissionen.

Befugnisse

(6026) Die Sicherheitsbehörden brauchen gleichwertige Befugnisse im Umgang mit dem Internet wie außerhalb des Internets. Das bedeutet im Einzelnen: Es darf für die Befugnisse der Polizei zu Eingriffen in das Fernmeldegeheimnis zum Schutz der Bevölkerung keinen Unterschied machen, ob die Nutzer sich zur Kommunikation der klassischen Telefonie oder klassischer SMS bedienen oder ob sie auf internetbasierte Messenger-Dienste ausweichen. Die Zusammenarbeit von Bund und Ländern bei der Cyberabwehr soll ausgebaut, verbessert und strukturell neu geordnet werden. Die Rolle des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird gestärkt.

(6036) Wo Strafbarkeitslücken bestehen, werden wir eine Strafbarkeit für das Betreiben krimineller Infrastrukturen einführen, um speziell im Internet eine Ahndung von Delikten z. B. das Betreiben eines Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen einzuführen. Wir wollen Angriffe aus dem Cyberraum gegen unsere kritischen Infrastrukturen abwehren und verhindern.

(6044) Wir wollen die Sicherheitsbehörden bei der Verfolgung und Prävention von Cyberkriminalität durch die Schaffung notwendiger rechtlicher, organisatorischer sowie technischer Rahmenbedingungen stärken.

(6048) Wir wollen, dass die Sicherheitsbehörden ihre bestehenden Befugnisse auch in der digitalen Welt anwenden und tatsächlich durchsetzen können.

Opferschutz

(6161) Wir werden alles Notwendige tun, um Kindesmissbrauch und Kinderpornografie möglichst zu verhindern und entschieden zu bekämpfen. Präventionsprogramme wie „Kein Täter werden" sind dabei ein wichtiges Element. Wir führen eine Strafbarkeit für den Versuch des Cybergroomings ein, um Kinder im Internet besser zu schützen und die Effektivität der Strafverfolgung pädophiler Täter, die im Netz Jagd auf Kinder machen, zu erhöhen.

Prävention

(6312) Wir betonen die Bedeutung der sozialwissenschaftlichen und kriminologischen Sicherheitsforschung, u. a. die hohe Relevanz von Dunkelfeldstudien und anderer empirischer Forschung z. B. zu organisierter Kriminalität, und wollen diese wissenschaftlichen Bereiche beim Bundeskriminalamt und in der wissenschaftlichen Forschung durch Universitäten und Dritte stärken.

(6318) Wir treten für eine evidenzbasierte Kriminalpolitik ein. Wir wollen, dass kriminologische Evidenzen sowohl bei der Erarbeitung von Gesetzentwürfen als auch bei deren Evaluation berücksichtigt werden. Wir unterstützen das unabhängige Deutsche Forum für Kriminalprävention. Um ein Gesamtbild der langfristigen Kriminalitätsentwicklung zu bekommen, streben wir eine zügige Aktualisierung des Periodischen Sicherheitsberichts an. Um die Aussagekraft der Strafrechtspflegestatistiken zu erhöhen, werden wir in Zusammenarbeit mit den Ländern ein Strafrechtspflegestatistikgesetz schaffen. Die Kriminal- und Strafrechtspflegestatistiken sollen langfristig zu einer Verlaufsstatistik zusammengeführt werden. Hierzu soll eine Machbarkeitsstudie in Auftrag gegeben werden.

(6329) Gerade im weiter wachsenden Bereich des islamistischen Extremismus und Terrorismus wollen wir Prävention und Deradikalisierung weiter stärken, national und auf EU-Ebene. Wir werden den radikalen Islam in Deutschland zurückdrängen. Wir erwarten, dass Imame aus dem Ausland Deutsch sprechen. Radikalisierte Moscheen werden wir beobachten und gegebenenfalls schließen. Hierzu werden wir die Praxis zwischen Bund und Ländern abstimmen.

6 Schlussfolgerungen für die Bürgerrechtspolitik für die nächsten 4 Jahre

Die aktuelle Hyperaktivität der Landesgesetzgeber im Sicherheitsbereich ist überraschend angesichts des Plans der neuen Bundesregierung, ein einheitliches Polizeigesetz in Form eines Musterentwurfes zu erarbeiten. Dass gerade Bayern mit übermäßigen Befugnissen vorprescht, spricht nicht dafür, dass diese Passage von allen Bundes-Koalitionspartnern wirklich ernst gemeint wäre. Aber auch die anderen derzeit hyperventilierenden Bundesländer preschen gegenüber den Bundesvorgaben vor, etwa wenn nicht der Pilotversuch zur Video-Mustererkennung abgewartet werden soll und diese Maßnahme allerorten in Entwürfen auftaucht. Tatsächlich erwiesen sich frühere Entwürfe für Musterpolizeigesetze als wenig hilfreich, da parteipolitische Präferenzen praktisch durchgängig Vorrang hatten vor dem Wunsch nach einheitlicher Regulierung.

Die Aussagen zur Sicherheitspolitik im Koalitionsvertrag sind relativ verwirrend und unsystematisch. Die Inhalte lesen sich weniger beängstigend als das, was die CDU, die CSU und die SPD derzeit auf Landesebene treiben: Bei der Videoüberwachung wird „Augenmaß" angekündigt. Selbst die Absicht, DNA-Phänotypisierung einzuführen, bewegt sich auf einem realistischeren Niveau als das, was etwa in Bayern und Baden-Württemberg schon auf den Weg gebracht worden ist bzw. wird. Jedenfalls scheint die SPD die allzu kühnen Überwachungswünsche von CDU/CSU nicht zugelassen zu haben. Beängstigend ist dagegen, dass im Kontext der

Erweiterung von Befugnissen das Thema Datenschutz nicht auftaucht; selbst Maßnahmen zur Wahrung der Grundrechte und der Rechtsstaatlichkeit werden allenfalls am Rande erwähnt.

Das Legitimationsmuster für die aktuellen Polizeirechtsreformen findet sich auch im Koalitionsvertrag: Es geht um die Bekämpfung des gewalttätigen Islamismus und des Terrorismus. Doch beschränkt sich der Koalitionsvertrag hierauf nicht; er anerkennt vielmehr neben dieser symbolhaften Entschiedensheitsgeste zugleich auch die realen Sicherheitsbedürfnisse der Menschen im Alltag (z. B. Bekämpfung von Wohnungseinbrüchen). Und selbst bei den neuen Feindbildern wird nicht nur auf härtere Strafen und massiveres Vorgehen gesetzt, sondern auch auf Ursachenforschung und Prävention.

Das mit dem Bayerischen Polizeigesetzentwurf versendete Signal ist ein doppeltes: Zum einen geht es darum, vor den bayerischen Landtagswahlen im Oktober 2018 die Hoheit über die Stammtische im Lande zurückzuerobern, die der CSU von der AfD streitig gemacht wird. Insofern kommt es der CSU sogar recht, dass die kritische Diskussion über das PAG inzwischen die Öffentlichkeit erreicht. Dass damit der CSU gedient wird, darf die inhaltliche Kritik nicht schmälern. Das andere Signal setzt der Bundesinnenminister, CSU-Chef und frühere bayerische Ministerpräsident auf Bundesebene. Er will die Richtung in der Sicherheitspolitik gegenüber den Koalitionspartnern bestimmen. Sein Gegengewicht bei der SPD, die Justizministerin Katarina Barley, dürfte – ähnlich wie zuvor Heiko Maas – dem liberalen Flügel ihrer Partei zugerechnet werden. Insofern wird im Bund nicht so heiß gegessen werden, wie in Bayern gekocht wird.

Doch sollte die Diskussion um die Vorratsdatenspeicherung abschreckendes Beispiel sein: Damals knickte Maas nicht nur vor dem CDU-Innenminister Thomas de Maizière ein, sondern insbesondere vor seinen Parteichef Sigmar Gabriel, der für Bürgerrechte wenig und für rigide Sicherheitspolitik viel übrig hatte. Andrea Nahles und Olaf Scholz, die beiden neuen starken Personen der SPD, haben sich mit Bürgerrechtsengagement bisher nicht profiliert; Scholz in Hamburg sogar eher durch das Gegenteil.

Dennoch sieht es so schlecht für die nächsten vier Jahre nicht aus: Wenn die SPD eines gelernt hat aus ihrer Wahlschlappe 2017, dann dass sie sich von Angela Merkel und der CDU/CSU auch bei anderen als den SPD-Herzensthemen nicht über den Tisch ziehen lassen darf, will sie nicht in der Mitte der Gesellschaft ihre Zustimmung verlieren. Es ist absehbar, dass die inhaltlichen politischen Debatten der nächsten vier Jahre weniger zwischen Regierung und Opposition ausgetragen werden (wenn die SPD zumindest das richtig macht), sondern zwischen ihr und der CDU/CSU. Es geht also darum, durch öffentlichen Druck die SPD dazu zu bringen, bürgerrechtliche Positionen zu vertreten.

Dabei sollten im Detail Schwarz-weiß-Debatten vermieden werden, welche die SPD zwingen, für eine der beiden Seiten „Farbe" zu bekennen. Wir müssen es also schaffen, dass nicht alle teilnahmslos auf das brennende Haus des Bürgerrechtsabbaus blicken, sondern dass die Medien sowie die öffentliche Meinung die SPD und die Bundestags-Oppositionsparteien dazu bringen, dass sie schon die Brandstiftung verhindern und in jedem Fall früher zur Stelle sind, als das Bundesverfassungsgericht als allerletzte Hilfe.

1 Gesetzentwurf zur Neuordnung des Polizeirechts (PAG-Neuordnungsgesetz) v. 30.01.2018, BayLT-Drs. 17/20425.

2 BVerG 03.03.2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999.

3 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419.

4 EuGH 08.04.2014 – C 293/12 u. C 594/12, NJW 2014, 2169.

5 EuGH 06.10.2015 – C-362/14, NJW 2015, 3151.

6 EuGH 13.05.2014 – C-131/12, NJW 2014, 2257.

7 BKA-G v. 25.12.2008, BGBl. I S. 2034.

8 G. v. 05.05.2017, BGBl I S. 1066.

9 G. v. 01.06.2017, BGBl I S. 1354.

10 G. v. 24.07.2017, BayGBVl 2017, 388.

11 G. v. 28.11.2017, BaWüGBl S. 631; dazu Busch, Bürgerrechte&Polizei November 2017/CILIP 114, 91 f. m. w. N.

12 Als Änderungsantrag zu einem Entwurf eines Landesverfassungsschutzgesetzes, LT-Drs. 5782 v. 14.12.2017.

13 Dazu der Beitrag von Freiheitsfoo in diesem Heft.

14 Dazu der Beitrag von Freiheitsfoo in diesem Heft.

15 Siehe dazu unten S. 29.

16 G. v. 17.11.2015, BGBl. I 1938.

17 G. v. 26.07.2016, BGBl I S. 1818.

18 G. v. 16.06.2017, BGBl I S. 1634 und G. v. 30.06.2017, Art. 2, BGBl I 2097, 2128 mit weiteren Änderungen zum SÜG, MAD-G, BND-G und Art. 10-G.

19 G. v. 23.12.2016, BGBl I S. 3346.

20 Zuletzt G. v. 06.03.2018, GV.NRW S. 144.

21 G. v. 08.08.2014, ThürGVBl S. 529.

22 G. v. 12.07.2016, BayGVBl S. 145.

23 G. v. 15.09.2016, NdsGVBl S. 194.

24 G. v. 28.11.2017, BaWüGBl S. 621.

25 HessLT-Drs. 19/5412 v. 14.11.2017; dazu Gössner, Stellungnahme v. 31.01.2018, https://ilmr.de/wp-content/uploads/2018/02/Goessner-StellgnahmeVS-GE-Hessen2-2018.pdf.

26 G. v. 10.12.2015, BGBl I 2015, 2218.

27 BVerfG 02.03.2010 – 1 BvR 258, 269 u. 586/06, NJW 2010, 833.

28 BVerfG 26.03.2017 – 1 BvR 3156/15 u. 1 BvR 141/16.

29 EuGH 21.12.2016 – C-203/15 u. C-698/15, RDV 2017, 29 = CR 2017, 225 = K&R 2017, 105.

30 Verfassungsgericht zweifelt an der Vorratsdatenspeicherung, www.faz.net 11.01.2018.

31 G. v. 17.08.2017, BGBl I S. 3202.

32 BT-Drs. 13/4438 v. 23.04.1996.

Bayern: Verfassungsklage gegen „drohende Gefahr“ bei Polizeibefugnissen

Die Grünen im Bayerischen Landtag haben beim Bayerischen Verfassungsgerichtshof (BayVerfGH) gegen das „Gesetz zur effektiveren Überwachung gefährlicher Personen („Gefährdergesetz“) Verfassungsklage eingelegt. Sie wenden sich vor allem dagegen, dass die Eingriffsschwelle für polizeiliche Aktionen auf eine „drohende Gefahr“ gesenkt werden soll. Gemäß Dr. Ino Augsberg, Jurist von der Universität Kiel, ist dieses Kriterium polizeilichen Handelns juristisches Neuland. Die Polizei kann laut dem seit August 2017 geltenden Gesetz im Vorfeld von befürchteten Gefährdungslagen handeln. Für eine drohende Gefahr muss keine Straftat begangen werden, es reicht aus, wenn die Wahrscheinlichkeit begründet ist, dass in überschaubarer Zukunft eine Straftat begangen wird. Ab wann beispielsweise von einem potenziellen Sexualstraftäter Gefahr droht und er mit einer elektronischen Aufenthaltsüberwachung überzogen werden kann, bleibt der polizeilichen Beurteilung überlassen. Auch wenn die Polizei die eingeräumten Möglichkeiten nicht voll ausschöpfen würde, so ändere, so Augsberg, das nichts an der fehlenden Bestimmtheit und der Unverhältnismäßigkeit: „So weit darf der Gesetzgeber die Auslegung seiner Gesetze nicht delegieren“. Neben der Organklage der Grünen liegen weitere Popularklagen gegen das „Gefährdergesetz“ vor, unter anderem eine der Jusos in Bayern.

In einer zweiten Novellierungsrunde zum Bayerischen Polizeiaufgabengesetz (BayPAG), zu dem am 20.03.2018 im Landtag die Expertenanhörung stattfand, marschiert die CSU weiter stramm in Richtung Präventiv- und Überwachungsstaat. Die Eingriffsbefugnisse bei „drohender Gefahr“ würden danach noch einmal deutlich erweitert. Statt mit einer aufwändigeren Fußfessel dürfte heimlich die Telekommunikation des als Gefährder Eingestuften künftig überwacht werden. Katharina Schulze, Fraktionsvorsitzende und innenpolitische Sprecherin der Grünen, kritisierte die damit verbundene „Vernachrichtendienstlichung“ der Polizei durch die Präventivbefugnisse. Sie befürchtet, dass Bayern als Experimentierfeld dient und der frischgebackene Bundesinnenminister Horst Seehofer die „drohende Gefahr“ für das Polizeirecht des Bundes zu übernehmen versucht. Sollte die zweite PAG-Novelle nicht mehr verändert werden, so kündigte sie an, „dann werden wir uns eben nochmal vor dem Bayerischen Verfassungsgericht treffen“. Seehofers Musterpolizeigesetz in ähnlicher Form wäre, so Augsberg, ein Fall fürs Bundesverfassungsgericht.

Diese zweite PAG-Novelle war am 14.03.2018 Gegenstand einer Anhörung im Innen- und Verfassungsausschuss. Der Landesbeauftragte für Datenschutz Thomas Petri stellte in den Raum, dass die vom Bundesverfassungsgericht geforderte „Überwachungsgesamtrechnung“, also ein umfassende Abwägung zwischen Freiheit und Sicherheit hinsichtlich aller bestehenden Kontrollbefugnisse, angesichts der vielen übermäßigen Eingriffsmöglichkeiten schon zur Verfassungswidrigkeit des Entwurfes führt. Auch andere Sachverständige bezeichneten die Vorschläge als verfassungswidrig oder „verfassungsrechtlich problematisch“ (dazu ausführlich S. 13).

Kritisch sehen sie unter anderem, dass die Polizei laut dem Gesetzentwurf in Zukunft einfacher Telefone überwachen oder auch Briefe öffnen darf als bisher, wobei auf die neue Kategorie der „drohenden Gefahr“ zurückgegriffen wird. Das Bundesverfassungsgericht (BVerfG) hat ausgeführt, dass es sinnvoll sein könne, wenn Behörden schon zu diesem Zeitpunkt tätig werden könnten, insbesondere bei Terrorgefahr. Die bayerische Staatsregierung will darüber hinausgehend die Polizei nicht nur bei Terrorgefahr präventiv tätig werden lassen, sondern auch dann, wenn ein „bedeutendes Rechtsgut“ in Gefahr ist. Dazu gehören Leben, Gesundheit und Freiheit, aber auch Dinge, deren Erhalt im besonderen öffentlichen Interesse ist. Gemäß Franz Schindler, Vorsitzender des Verfassungsausschusses und bei der SPD, greift das Gesetz auch bei „normaler Kriminalität“. Der Polizei stehe dann das ganze „Schreckensszenario“ der Überwachung offen. Darunter fallen unter anderem die Onlinedurchsuchung, die Überwachung von Telefon und Handy oder der Post. Zudem kann aufgrund von Funkzellendaten ein Bewegungsprofil erstellt werden. Für Schindler ist es keine große Hürde, dass die Erlaubnis eines Richters eingeholt werden muss, was regelmäßig erst hinterher stattfände.

Markus Löffelmann, Richter am Landgericht München, verbindet mit der Einführung der Kategorie der „drohenden Gefahr“ eine „nicht mehr akzeptable Herabsetzung der polizeilichen Eingriffsschwelle“. Markus Möstl, der den Lehrstuhl für öffentliches Recht an der Universität Bayreuth innehat, meinte dagegen, die Staatsregierung bewege sich auf „verfassungsrechtlich sicherem Boden“.

Grüne und SPD sehen in einer Polizei, die immer mehr im Verborgenen agiert, eine große Gefahr. Die Zuständigkeiten von Verfassungsschutz und Polizei dürften nicht immer mehr verschwimmen, sagt Schulze. Schindler mahnt, dass sich der Gesetzgeber beim Trennungsgebot von Verfassungsschutz und Polizei schon etwas gedacht habe.

Auf Kritik der Opposition, aber auch einiger Experten, stößt eine weitere Regelung zu DNA-Analysen. Innenminister Herrmann erklärt ihre Sinnhaftigkeit meist mit folgendem Beispiel: Die Polizei entdeckt die Werkstatt eines potenziellen Bombenlegers. Der aber ist gerade nicht da, seine DNA-Spuren vielleicht schon. Zukünftig soll die Polizei genetisches Material sicherstellen und es wie ein Phantombild verwenden können. Herkunft, Haarfarbe, Geschlecht, Augenfarbe, all das soll aufgenommen werden. Sehr viel zuverlässiger als eine Zeichnung, die auf der Grundlage von

Zeugenaussagen angefertigt wurde, argumentieren die einen. Der bayerische Landesbeauftragte für Datenschutz Thomas Petri aber kritisiert einen „erheblichen Eingriff in das informationelle Selbstbestimmungsrecht". Sensible Daten aufzunehmen, obwohl noch nicht einmal ein Gefahrenverdacht besteht, nannte der Sachverständige Kurt Graulich, ehemaliger Richter am Bundesverwaltungsgericht, „nicht nachvollziehbar" (dazu ausführlich S. 19).

Ähnlich besorgt zeigt sich Petri bei dem geplanten Einsatz von intelligenter Videoüberwachung wie sie vor kurzem bei einem Pilotversuch am Berliner Bahnhof Südkreuz getestet wurde. Unter dem Vorbehalt der „drohenden Gefahr" dürfte dann ein Gesichtserkennungssystem eingesetzt werden, um etwa mögliche Terroristen aus der Menschenmenge herauszufiltern. Gibt es keine Treffer, werden die Daten nicht gespeichert. Bei Pilotprojekten zeigte sich, dass die Trefferquote bei Tageslicht bei um die 60% liegt, bei abnehmendem Licht sank sie auf zehn bis 20%. Katharina Schulze zweifelte den Nutzen dieser Maßnahme an. Gebe es aber doch mal einen Treffer und die Polizei habe einen Erfolg, hört Schindler schon den Ruf, die Daten doch zu speichern: „Was technisch möglich ist, wird gemacht".

Der Entwurf für die zweite PAG-Novelle umfasst über 100 Seiten. Selbst die Experten merkten an, dass die Materie komplex sei. Mehr als zweieinhalb Stunden blieben den Experten nicht, um bei der Anhörung ihre Bedenken darzulegen, bei der auch noch ein anderes Gesetz besprochen wurde. Dies war für Schindler „eine Farce" und Schulze ergänzte: „Das sind tiefe Eingriffe in die Bürgerrechte, für die ein Parlament mehr Zeit haben sollte".

Nachdem die erste PAG-Novelle in Bayern, bei der die „drohende Gefahr" eingeführt wurde, fast ohne mediale Resonanz blieb, formiert sich spät, aber heftig Widerstand gegen den die nunmehr geplante totalitäre Totalrenovierung des Polizeirechts. Dies veranlasste Bayerns Innenminister Joachim Herrmann (CSU), eine Desinformationskampagne in sozialen Netzwerken gegen das geplante neue Polizeigesetz zu beklagen. Es gebe offenbar einige, die „mit falschen Behauptungen gezielt Stimmung" gegen die Gesetzesnovelle machten". Die vielfach geäußerte Kritik, die Polizei dürfe in Bayern vom Sommer 2018 an ohne konkreten Verdacht gegen Bürger ermitteln und Daten auslesen, sei „völlig aus der Luft gegriffen". Herrmann widersprach der Darstellung, die Freiheitsrechte sollten eingeschränkt werden. Der Einsatz von verdeckten Ermittlern sei bisher schon möglich gewesen. „Zukünftig ist in vielen Fällen ein Richtervorbehalt vorgesehen, den es bisher noch nicht gab." Die Formulierung, Bayern schaffe das „härteste Polizeigesetz seit 1945", bezeichnete der Innenminister als „blanken Unsinn". „1945 gab es noch keine Terroristen, die mit dem Smartphone agierten oder sich über das Internet verabredeten", so Herrmann.

Sowohl beim Bayerischen Verfassungsgerichtshof als auch in Karlsruhe sind darüber hinaus Klagen gegen das Bayerische Verfassungsschutzgesetz von verschiedenen Parteien anhängig (CSU verteidigt Polizeigesetz; *Ermert*, Grüne legen Verfassungsbeschwerde gegen bayerisches „Gefährdergesetz" ein, www.heise.de 29.03.2018; Schnell, Bayern will die Befugnisse der Polizei massiv ausweiten, www.sueddeutsche.de 20.03.2018).

Presseerklärung der DVD vom 05.04.2018

Deutsche Vereinigung für Datenschutz warnt vor Totalüberwachung durch Verschärfung des bayerischen Polizeirechts

Im Bayerischen Landtag steht derzeit ein Entwurf für das Polizeiaufgabengesetz (PAG) zur Diskussion, der die schlimmsten Befürchtungen von Bürgerrechtlern übertrifft. Darin wird die Ausweitung polizeilicher Befugnisse zur Erhebung personenbezogener Informationen in einem Maße vorangetrieben, das nach Ansicht der Deutschen Vereinigung für Datenschutz e. V. (DVD) die vom Bundesverfassungsgericht gesetzten absoluten Grenzen zu einer „flächendeckenden vorsorglichen" Überwachung überschreitet. Das geplante Gesetz weitet sowohl die personale wie auch die digitale technische Überwachung aus, vom Einsatz von verdeckten Ermittlern über die Telekommunikationsüberwachung und die „Durchsuchung" von informationstechnischen Systemen bis hin zum Einsatz polizeilicher Bodycams in Wohnungen, von Drohnen sowie bis hin zu Genanalysen zu bestimmten Körpermerkmalen und zur „biogeografischen Herkunft".

In einer juristischen Stellungnahme (s. u. S. 13) stellt die DVD fest, dass die bewährten rechtlichen Grundlagen des bestehenden deutschen Polizeirechts schon dadurch verlassen werden, dass bei einer Vielzahl von Befugnissen nicht mehr eine konkrete Gefahr gefordert wird, sondern eine drohende Gefahr genügt, also eine Situation, in der nach polizeilicher Bewertung eine Gefahr entstehen könnte. Erfasst werden nicht nur Störer und unvermeidbar betroffene Dritte, sondern auch solche Personen, die „mutmaßlich" mit diesen in Verbindung stehen.

DVD-Vorstandsmitglied Thilo Weichert: „Künftig benötigt die Polizei nicht

mehr Fakten; es genügen Mutmaßungen. Verdächtigungen und Spekulationen sollen also künftig das polizeiliche Handeln leiten können." Damit einher gehen Eingriffsbefugnisse, die unterschiedslos viele Menschen betreffen wie z. B. die Videoüberwachung. Dabei wird nicht nur auf klassische Kameratechnik zurückgegriffen; möglich sein soll auch der Einsatz von Drohnen oder von so genannter Musterkennung. Thilo Weichert: „Die Regelung zur Mustererkennung ermöglicht es der Polizei, technisch Menschen aus einer Menschenmenge als verdächtig herauszufischen, nur weil sie als verdächtig programmierte Eigenschaften haben. Damit wird der digitalisierten Willkür und der Diskriminierung von Minderheiten die Tür geöffnet. Dies trifft auch für die Erstellung sog. genetischer Phantombilder zu. Diese Techniken befinden sich noch in einem Entwicklungsstadium, das mehr Fehler als polizeiliche Hilfe produziert."

Werner Hülsmann, stellvertretender DVD-Vorsitzender: „Lägen der CSU-Mehrheit unser Grundgesetz und insbesondere unsere Grundrechte am Herzen, so dürfte dieses Gesetz nicht verabschiedet werden. Der bisherige Ablauf der Gesetzgebung – übereilt und ohne inhaltliche öffentliche Diskussion – lässt das Schlimmste befürchten. Das Gesetz gehört in vielen Einzelteilen und in seiner Gesamtheit auf den rechtlichen Prüfstand, um Schlimmes in der Zukunft zu verhindern."

Stellungnahme der Deutschen Vereinigung für Datenschutz e. v. (DVD) zum Gesetzentwurf der Staatsregierung zur

Neuordnung des Bayerischen Polizeirechts

(PAG-Neuordnungsgesetz) vom 30.01.2018, BayLT-Drs. 17/20425

Vorbemerkung

Der Entwurf zur Novellierung des Polizeiaufgabengesetzes (PAG-E) soll, so die Begründung, europäische sowie verfassungsrechtliche Vorgaben, insbesondere aus der Richtlinie (EU) 2016/680 zum Datenschutz bei Polizei und Justiz vom 27.04.2016 (künftig DSRl-JI – Datenschutzrichtlinie Justiz/Inneres), sowie die befugniseinschränkende Rechtsprechung des Bundesverfassungsgerichts (BVerfG), insbesondere die umfassenden Festlegungen zum Bundeskriminalamtsgesetz,[1] umsetzen. Tatsächlich werden bei dieser Gelegenheit viele **neue polizeilichen Befugnisnormen** vorgeschlagen zwecks „dem Stand der Technik entsprechender Ergänzung und noch effektiveren Ausgestaltung" (S. 1).

Die vorliegende Stellungnahme befasst sich nicht mit sämtlichen geplanten Neuregelungen, sondern greift diejenigen heraus, die aus Sicht der DVD hinsichtlich des Schutzes der informationellen Selbstbestimmung der Menschen besonders problematisch sind. Von den Änderungsvorschlägen betroffen ist nicht nur das Grundrecht auf Datenschutz (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 GRCh), sondern in Fällen des Zugriffs auf private informationstechnische (IT-) Systeme das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[2], sowie bei vielen Maßnahmen das Telekommunikationsgeheimnis (Art. 10 GG, Art. 7 GRCh), das Recht auf Schutz der Wohnung (Art. 13 GG, Art. 7 GRCh) sowie weitere informationelle Grundrechte.[3]

Nicht näher behandelt werden u. a. folgende neue, auch **verfassungsrechtlich problematische Befugnisnormen**:

- die Möglichkeit einer polizeilichen Meldeanordnung (Art. 16 Abs. 2 Nr. 2 PAG-E),[4]
- die Herabsenkung der Eingriffsschwelle beim Betreten und Durchsuchen von Wohnungen durch Ersetzen des Begriffs der gegenwärtigen Gefahr durch den der dringenden Gefahr (Art. 23 Abs. 1 Nr. 3 PAG-E),[5]
- die Ausweitung der Befugnisse für Aufgaben der Grenzkontrolle und Sicherung von Anlagen (Art. 29 PAG-E),[6]
- die Ausweitung der Befugnis zur Verarbeitung besonderer Kategorien personenbezogener Daten ohne eine unbedingte Erforderlichkeit oder Grundrechtsgarantien vorzusehen (Art. 30 Abs. 2 PAG-E),[7]
- die Datenerhebung zu Zwecken des Personenschutzes ohne Erfordernis einer Zustimmung des Betroffenen (Art. 32 Abs. 1 S. 1 Nr. 1b, 61 Abs. 1 PAG-E),[8]
- die Erstellung und Aufzeichnung von Bild und Ton bei öffentlichen Veranstaltungen und von Videos bei Anhaltspunkten für Straftaten und erheblichen Ordnungswidrigkeiten sowie von Übersichtsaufnahmen (Art. 33 Abs. 1 PAG-E).[9]
- der Einsatz von sog. Bodycams zum Schutz eines bedeutenden Rechtsguts (Art. 33 Abs. 4 S. 1 PAG-E),[10]
- die Weiterung der erst jüngst eingeführten elektronischen Aufenthaltsüberwachung (Art. 34 PAG-E),[11]
- die Postsicherstellung bei mutmaßlichem Gefahrenbezug auch bei einem Nachrichtenmittler (Art. 35 Abs. 1 PAG-E),[12]
- die Übertragung der Befugnis zur Postöffnung an die Polizei (Art. 35 Abs. 4, 5 PAG-E),[13]
- die Ausweitung der Fristen für den Einsatz verdeckter Ermittler (Art. 37 Abs. 2, 3 PAG-E),[14]
- der Einsatz von Vertrauenspersonen als Standard- und nicht als absolute Ausnahmemaßnahme (Art. 38 Abs. 2 PAG-E),[15]

- die Ausweitung der Befugnis zur polizeilichen Beobachtung (Art. 40 PAG-E),[16]
- die Ausweitung der Befugnis zur Funkzellenabfrage, ohne aber eine klare Regelung vorzunehmen (Art. 43 PAG-E),[17]
- die Zulassung der Online-Durchsuchung schon bei einer drohenden Gefahr bestimmter Rechtsgüter (Art. 45 PAG-E).[18]

Dies erfolgt unter
- ungenügendem Schutz von Berufsgeheimnissen sowie des Kernbereichs privater Lebensgestaltung (Art. 49 PAG-E),[19]
- unter ungenügender parlamentarischer sowie öffentlicher Unterrichtung und Kontrolle (Art. 52, 58 Abs. 6 PAG-E),[20]
- ungenügender unabhängiger richterlicher Kontrolle (Art. 53, 92 Abs. 3 PAG-E),[21]
- unter unzureichender Beachtung der verfassungsrechtlich begründeten Löschpflichten (Art. 54 PAG-E)[22] und
- unter übermäßiger Beschränkung des Auskunftsanspruch von Betroffenen (Art. 65 Abs. 2 PAG-E).[23]

Nicht vertieft behandelt werden hier die geplanten Regelungen zur **DNA-Analyse** (DNA-Identifizierung, DNA-Phänotypisierung, Art. 14 Abs. 3, 32 Abs. 1 S. 2 u. 3 PAG-E). Hierzu wurde vom Netzwerk Datenschutzexpertise eine ausführliche Stellungnahme erarbeitet, die zu dem Ergebnis kommt, dass die geplanten Regelungen gegen europäisches und nationales Verfassungsrecht sowie gegen die europarechtlichen Vorgaben der DSRl-JI verstoßen. Grund für diese Bewertung ist, dass nicht erforderliche und unverhältnismäßige Maßnahmen mit einem hohen Diskriminierungsrisiko erlaubt werden sollen, ohne dass Schutzvorkehrungen vorgesehen sind. Zudem fehle es insofern weitgehend an einer Gesetzgebungskompetenz des Bundeslandes.[24] Die DVD schließt sich dieser Bewertung an.

Der Gesetzentwurf macht eine Vielzahl weiterer polizeilicher Maßnahmen von einer **drohenden Gefahr** (elektronische Aufenthaltsüberwachung, Art. 15 Abs. 3 Nr. 1, Bestandsdatenauskunft, Art. 43 Abs. 5 S. 1), evtl. für bedeutende Rechtsgüter (Verarbeitung von besonderen Kategorien personenbezogener Daten, Art. 30 Abs. 2 Nr. 2a, Mustererkennung, Art. 33 Abs. 5 S. 2, Postsicherstellung, Art. 35 Abs. 1 Nr. 1, besondere Mittel der Datenerhebung, Art. 36, polizeiliche Beobachtung, Art. 40 Abs. 1 Nr. 2, Telekommunikationsüberwachung, Art. 42 Abs. 1 Nr. 1, Abs. 4 Nr. 1, Zugriff auf IT-Systeme, Art. 45 Abs. 1 Nr. 1, Übermittlung an Geheimdienst, Art. 60 Abs. 3 Nr. 1), abhängig. Dabei wird auf die erst jüngst vorgenommene Einführung dieser Eingriffsschwelle in Art. 11 Abs. 3 S. 2 Nr. 1-5 PAG Bezug genommen, die selbst den Schutz von „erheblichen Eigentumspositionen" einschließt. Mit Eingriffsbefugnissen bei „drohender Gefahr" werden Polizeibefugnisse ins Vorfeld einer Gefahr verlegt, also zu einem Zeitpunkt, in dem noch keine Gefahr besteht, sondern nach Ansicht der Polizei eine Gefahr entstehen könnte. Diese Vorverlagerung von Eingriffsbefugnissen hat das BVerfG bei drohenden terroristischen Straftaten zugelassen, nicht aber etwa bei Bedrohungen „erheblicher Eigentumspositionen".[25] Eine derartige Ausweitung von polizeilichen Standardbefugnissen ist zu unbestimmt und unverhältnismäßig.[26]

Ähnlich problematisch wie die Ausweitung von Befugnisnormen auf (noch) nicht bestehende Gefahren (s. o.) ist die Anknüpfung an Personen und Sachverhalte, die „**mutmaßlich** in Zusammenhang mit der Gefahrenlage stehen" (so z. B. Postsicherstellung beim Nachrichtenmittler, Art. 35 Abs. 1 S. 1 Nr. 2 PAG-E, der Einsatz besonderer Mittel der Datenerhebung gegenüber Kontakt- und Begleitpersonen, Art. 36 Abs. 2 PAG-E, polizeiliche Beobachtung, Art. 40 Abs. 1 Nr. 3 Abs. 2 PAG-E; Telekommunikationsüberwachung Art. 42 Abs. 1 Nr. 2b PAG-E, Eingriff in IT-Systeme, Art. 45 Abs. 1 S. 1 Nr. 2 PAG-E). Dabei greift der Entwurf die grundsätzliche Zulassung polizeilicher Maßnahmen gegenüber Kontakt- und Begleitpersonen auf und entgrenzt die Befugnisse, indem an Stelle einer tatsächlichen Nähe zur Gefahr eine mutmaßliche Nähe genügen soll.[27] Tatsächlich enthält die Rechtsprechung des BVerfG, anders als die Begründung an mehreren Stellen suggeriert (S. 54, 59, 62, 66), keine Rechtfertigung von Eingriffen ausschließlich auf der Grundlage von Mutmaßungen.

Durchsuchung elektronischer Speichermedien

Art. 22 Abs. 2 S. 1 PAG-E erlaubt die Durchsuchung von elektronischen Speichermedien, soweit von einem Durchsuchungsobjekt, also einem körperlichen Gegenstand, „auf sie zugegriffen werden kann". Bei einer derartigen „Durchsuchung" kann es zu Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kommen.[28] Die Regelung enthält keine Vorkehrungen, um Verletzungen des Kernbereichs privater Lebensgestaltung oder den Zugriff auf Daten, die dem Zeugnisverweigerungsrecht nach den §§ 53, 53a StPO unterliegen, zu verhindern. Eine systematische Durchsuchung und **digitale Auswertung** von Festplatten und Cloudinhalten kann nicht mit einer Durchsuchung von körperlichen Sachen gleichgesetzt werden. Die Eingriffsintensität liegt erheblich höher. Dies hat zur Folge, dass zusätzliche Sicherungsmaßnahmen vorgesehen werden müssen, etwa die Regelung eines Richtervorbehalts, die Pflicht zur Protokollierung der Auswertungsmaßnahmen oder die zur Benachrichtigung der Betroffenen.[29]

Bild- und Tonaufnahmen in Wohnungen

Art. 33 Abs. 4 S. 2 PAG-E sieht vor, dass offene Bild- und Tonaufnahmen, etwa durch **polizeiliche Bodycams**, in Wohnungen erstellt und gespeichert werden dürfen „zur Abwehr einer dringenden Gefahr für Leben, Gesundheit oder Freiheit einer Person", „sofern damit nicht die Überwachung der Wohnung verbunden wird". Damit erfolgt nicht nur ein Eingriff in das Recht auf informationelle Selbstbestimmung, ins Recht am eigenen Bild und ins Recht am eigenen Wort (Art. 2 Abs. 1 i. V. m. Art. 1 GG) bzw. ins Grundrecht auf Datenschutz (Art. 8 GRCh), sondern auch ein Eingriff in die Unverletzlichkeit der Wohnung (Art. 13 GG, Art. 7 GRCh). Betroffen sind nicht nur Störer, sondern auch mehr oder weniger unbeteiligte Dritte sowie die Poli-

zeibeamten. Die Regelung enthält keine Eingrenzung in Bezug auf besondere Räumlichkeiten, etwa für Psychologen-, Arzt- oder Anwaltspraxen.

Die **Eignung** der Maßnahme für Gefahrenabwehrzwecke ist äußerst umstritten und von einer Vielzahl von Rahmenbedingungen abhängig. Von der Maßnahme können nicht nur disziplinierende, sondern auch aggressionsfördernde Wirkungen ausgehen.[30]

Die geplante Regelung ist eindeutig verfassungswidrig, da sie nicht, wie in Art. 13 Abs. 4 GG vorgesehen, zwingend einen Richtervorbehalt vorsieht. **Art. 13 Abs. 4 GG** regelt nicht nur heimliche, sondern auch offene akustische wie optische Überwachungsmaßnahmen, etwa durch Videokameras, Infrarotkameras oder Mikrophone. Der im Entwurfstext vorgesehene Zusatz „sofern damit nicht die Überwachung der Wohnung verbunden wird", ändert an dieser klaren Zuordnung nichts, da begriffsnotwendig jeder Kameraeinsatz in einer Wohnung zugleich auch eine Überwachung der Wohnung darstellt. Dass mit der Überwachung vorrangig ein anderes Ziel verfolgt wird, spielt für die Anwendung der objektiv formulierten Anforderungen an Eingriffe in das Wohnungsgrundrecht keine Rolle. Das Wohnungsgrundrecht soll einen Rückzugsraum für die Menschen sicherstellen, der mit jeder Form der optischen oder akustischen Erfassung verletzt wird. Das Grundrecht soll dem Einzelnen gerade in seiner Wohnung zusichern, in Ruhe gelassen zu werden. Dieser Schutz darf nicht durch Abwägung mit Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden.[31]

Ein Rückgriff auf **Art. 13 Abs. 5 GG**, der als Ausnahme vorsieht, dass der Einsatz „ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen" dient, ist hier nicht möglich, da weder der Gesetzeswortlaut noch die Intention diesen ausschließlichen Schutz als einzigen Zweck im Auge hat.[32] Geschützt werden sollen nicht nur in der Wohnung tätige, sondern auch dritte Personen.

Anders als die Gesetzesbegründung (S. 88) behauptet, kann auch nicht **Art. 13 Abs. 7 GG** als Legitimation herangezogen werden. Danach dürfen Eingriffe „im Übrigen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung ... vorgenommen werden". Wegen der abschließenden Regelung in Art. 13 Abs. 4 GG kommt ein Rückgriff auf den subsidiären Art. 13 Abs. 7 GG nicht mehr in Betracht.

Der Verzicht auf einen Richtervorbehalt wird in der Gesetzesbegründung hinsichtlich der weiteren Verwendungen der Aufnahmen **„zu Strafverfahrenszwecken"** damit gerechtfertigt, dass diese „ohnehin umfassender richterlicher Kontrolle unterliegen" (S. 89). Dabei wird fälschlich davon ausgegangen, dass ein Strafrichter grds. die Zulässigkeit von Ermittlungsmaßnahmen überprüft; tatsächlich gilt dies nur für die Verwertbarkeit als Beweismittel, wobei andere rechtliche Kriterien gelten.

Optische und akustische Mustererkennung

Gemäß Art. 33 Abs. 5 PAG-E dürfen bei offenen Bild- und Tonaufnahmen im öffentlichen Raum (nicht beim Bodycam-Einsatz) „Systeme zur automatischen Erkennung und Auswertung von Mustern" zur Erkennung von Sachen und Personen eingesetzt werden, soweit dies erforderlich ist. Insofern stellte sich zunächst die Frage nach der **Geeignetheit** dieser Maßnahme. Bisherige Tests konnten diese mit den heute zum Einsatz kommenden Techniken nicht nachweisen und scheiterten z. B. bei Bildaufnahmen an den Lichtverhältnissen, an der Dynamik der Bilder sowie am Verbergen der identifizierenden Merkmale.[33]

Soweit über die Mustererkennung eine biometrische Identifizierung erfolgen soll, ist Art. 10 DSRl-JI zu beachten, da **„biometrische Daten zur eindeutigen Identifizierung"** als sensitive Daten bewertet werden (vgl. Art. 3 Nr. 13 DSRl-JI), so dass eine „unbedingte" Erforderlichkeit bestehen muss und „geeignete Garantien" vorgesehen werden müssen. Derartige Anforderungen bzw. Garantien enthält der Entwurf aber nicht. Der Verweis auf Art. 39 Abs. 3 S. 1, 2 u. 4 PAG-E, der eine unverzügliche Löschung nach Durchführung des Datenabgleichs ohne Treffer vorsieht, genügt nicht, da zunächst eine verdachtslose Erfassung aller Betroffenen erfolgt. Die spezifischen Risiken der Maßnahme, etwa von Falscherkennungen (false positives), werden nicht adressiert.

Die Maßnahme begründet einen schweren Eingriff und hat eine große Streubreite. Insofern wären hohe Anforderungen an Bestimmtheit und an die Eingriffsschwelle zu stellen.[34] Die Regelung ist zu **unbestimmt**, da sie sich nicht auf die Erkennung besonderer Muster (z. B. Gesichtserkennung) beschränkt, sondern über sämtliche biometrische Identifikatoren hinaus jede Form der Mustererkennung erfasst. Dazu gehören z. B. die Erkennung am Gang oder sonstiger Bewegungen. Dazu gehören letztlich auch Detektionen „auffälligen Verhaltens" von Einzelpersonen wie auch von Menschengruppen per Algorithmus. Da nicht nur Bild-, sondern auch Tonaufnahmen ausgewertet werden können sollen, erfasst die Formulierung sogar die inhaltliche Mustererkennung von Gesprächen. Eine andere Form der Mustererkennung ist die Detektion von bestimmten als gefährlich oder kriminell programmierten Merkmalen von Personen (z. B. Hautfarbe). So wird mit der Regelung eine Rechtsgrundlage geschaffen zur Diskriminierung und Stigmatisierung von Gruppen, die solche Merkmale aufweisen, ohne dass hiergegen angemessene Garantien im Gesetz vorgesehen sind.

Die vorgesehene Mustererkennung stellt eine **automatisierte Entscheidungsfindung im Einzelfall** dar, die in Art. 11 DSRl-JI geregelt ist. Gemäß Art. 11 Abs. 3 DSRl-JI sind Diskriminierungen durch profiling anhand von sensitiven Daten wie biometrischen Identifikatoren oder per Mustererkennung erfassten Daten zum Gesundheitszustand absolut verboten. Gemäß Art. 3 Nr. 4 DSRl-JI ist „Profiling" „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, In-

teressen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.[35] Auch andere Garantien und „zumindest das Recht auf persönliches Eingreifen seitens des Verantwortlichen“, sind nicht, wie in Art. 11 DSRl-JI gefordert, im PAG-E vorgesehen. Weiterhin fehlt es an einer Zweckbeschränkung auf die Gefahrenabwehr und die Strafverfolgung.

Anstatt dass **materiell-rechtlich** hohe Hürden für den Einsatz der Biometrie vorgesehen werden, wird die Mustererkennung als Standardmaßnahme für jede Form der Gefahrenabwehr und darüberhinausgehend sogar als Maßnahme gegen drohende Gefahren zugelassen. Der Verzicht auf eine darüber hinausgehende Beschränkung, etwa auf „im Einzelfall bestehende Gefahren für Leib und Leben“, macht die Regelung unverhältnismäßig und damit unzulässig.[36]

Verdeckter Zugriff auf informationstechnische Systeme

Gemäß Art. 45 Abs. 1 S. 1 Nr. 2 PAG-E wird der verdeckte Zugriff auf **informationstechnische (IT-) Systeme** von Dritten, also nicht nur von (drohenden) Störern erlaubt, soweit Umstände bestehen, dass diese „mutmaßlich“ die Systeme nutzen bzw. genutzt haben. Der Zugriff soll verdeckt mit technischen Mitteln erfolgen können. D. h., dass sich die Polizei als Hacker bei Dritten betätigen darf. Hinsichtlich des Hacking-Objektes erfolgt keine weitere Eingrenzung. Erfasst werden sollen nicht nur Geräte, d. h. Hardware von Personen, die zur (drohenden) Gefahr in Zusammenhang gebracht werden, sondern auch Software-Angebote bzw. Applikationen. Damit eröffnet die Regelung den Zugriff auch auf Plattformen wie Facebook oder Google sowie bei Cloud-Datenverarbeitern. Durch die Erlaubnis der Zugriffs auf Zugangsdaten und gespeicherte Daten besteht auch inhaltlich keine Eingriffsbeschränkung (s. o. zu Art. 22 PAG-E). Die Regelung ist zu unbestimmt und zugleich viel zu weit und dadurch unverhältnismäßig.

Einsatz von Drohnen

Art. 47 PAG-E erlaubt den Einsatz unbemannter Flugsysteme für „offene Bild- und Tonaufnahmen“, zur **technischer Erhebung von sonstigen Daten**, etwa aus der Telekommunikation sowie aus IT-Systemen. Mit dieser Befugnis werden Eingriffe in eine Vielzahl von Grundrechten, u. a. auch in das Telekommunikations- und das Wohnungsgrundrecht erleichtert. Spezifische Sicherungs- oder Schutzmaßnahmen sieht die Regelung nicht vor.[37]

Ein Spezifikum von Drohneneinsätzen besteht darin, dass von der Datenerhebung z. B. durch Videoüberwachung nicht nur Störer, sondern typischerweise auch viele völlig **Unbeteiligte betroffen** sind. Eine gezielte Unterscheidung bzgl. der Betroffenen ist zumeist nicht möglich. Damit wird eine verhaltenslenkende und von der Grundrechtswahrnehmung abschreckende Wirkung mit großer Streubreite erreicht, die hohe Schutzvorkehrungen nötig macht, die aber nicht vorgesehen sind.[38]

Der Gesetzestext suggeriert, dass es sich beim Drohneneinsatz nach Absatz 1 Nr. 1 um eine **offene Maßnahme** handeln würde. Relativierend wird in Art. 47 Abs. 2 S. 2 der Hinweis auf die Maßnahme nur als Sollvorschrift formuliert. Tatsächlich ist ein Hinweis oft überhaupt nicht möglich. So können polizeiliche von privaten oder sonstigen Drohnen in der Entfernung weder optisch noch akustisch unterschieden werden. Je größer die Entfernung, umso geringer ist die Wahrscheinlichkeit, dass Drohnen überhaupt als solche erkannt werden. Moderne Sensortechnik ermöglicht es inzwischen, aus großen Entfernungen die gewünschten Datenerhebungen durchzuführen; mit großen Entfernungen kann zugleich der sensorische Erfassungsraum massiv ausgeweitet werden.

Dass es sich beim Drohneneinsatz i. d. R. um einen **verdeckten Einsatz** handelt, ist auch der Regelung selbst zuzuschreiben, die sich nicht auf Bildaufnahmen beschränkt, sondern auch Tonaufnahmen vorsieht sowie elektronische Formen der Datenerfassung. Die Heimlichkeit des Informationsangriffs wird dadurch verstärkt, dass die Betroffenen heute grundsätzlich nicht mit einer Datenerfassung aus der Luft rechnen, etwa wenn per Drohne ein Späh- und Lauschangriff durch Fenster auf eine Wohnung erfolgt. Selbst bei Erkennung der Maßnahme ist wegen des flächenabdeckenden Ansatzes insbesondere im öffentlichen Raum ein Sichentziehen oft überhaupt nicht mehr möglich.[39]

Ist kein Späh- und Lauschangriff auf eine Wohnung geplant und wäre dieser auch materiell-rechtlich nicht zulässig, so gewährleistet die Regelung nicht, dass ein solcher Angriff auch nicht erfolgt, indem bei der Datenerhebung über Fenster in **Wohnungen** eingedrungen wird oder dass von oben vom Boden nicht einsehbare, zur Wohnung gehörende Bereiche erfasst werden.

Die Kombination des Drohneneinsatzes mit anderen Datenerhebungs- und Auswertungsbefugnissen, etwa der Mustererkennung, eröffnet Überwachungspotenziale von orwellschem Ausmaß und totalitärer Qualität. Die Regelung ist somit zu unbestimmt und greift in unverhältnismäßiger Form und ohne die nötigen Schutzvorkehrungen in eine Vielzahl von Grundrechten ein und ist **verfassungswidrig**.

Überwachungsgesamtrechnung

Der Gesetzentwurf enthält in seiner Gesamtheit von informationellen Eingriffsbefugnissen Erlaubnisse zur Überwachung der Bevölkerung, die über das vom BVerfG erlaubte Maß hinausgehen. Das BVerfG hat dargelegt, dass eine Gesetzgebung, „die auf eine möglichst **flächendeckende vorsorgliche Speicherung** aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte, ... von vornherein mit der Verfassung unvereinbar“ ist.[40] Es muss sichergestellt werden, dass nicht alle Aktivitäten der Bürgerinnen erfasst und rekonstruiert werden können. „Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem ´additiven` Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt“.[41] Diesen grundsätzlichen verfassungsrechtlichen Anforderungen genügt der Entwurf nicht. Er enthält Ermittlungsbefugnisse weit im Vorfeld von Gefahren sowie gegenüber jedermann und schöpft dabei die

technischen Möglichkeiten der Überwachung weitestgehend aus, ja sieht teilweise sogar Überwachungsmaßnahmen vor, die technisch heute noch nicht machbar sind, ohne adäquate Grundrechtssicherungen vorzusehen.[42]

Ergebnis

Der Entwurf für eine Neuordnung des bayerischen Polizeiaufgabengesetzes ist **in seinem gesamten Regelungsinhalt verfassungswidrig**. Die mit ihm vertiefte Abkehr von den Anforderungen an eine konkrete Gefahr als Anlass und einen Störer als Adressat der Maßnahmen eröffnet es der Polizei ohne adäquate Einschränkungen personenbezogene Daten zu erheben und damit in Grund- und Freiheitsrechte einzugreifen. Dabei wird oft weder die Eignung, geschweige die (unbedingte) Erforderlichkeit für die Gefahrenabwehr dargelegt und zur Voraussetzung gemacht. Selbst noch nicht bestehenden technischen Möglichkeiten wird für die Zukunft die Tür geöffnet, ohne dass Erfahrungen mit diesen gesammelt und deren Risiken bewertet werden konnten. Letztlich signalisiert der Entwurf an die Polizei: Alles ist möglich. Dies hat zur Folge, dass die Menschen begründet befürchten müssen, dass auch Alles gemacht wird und dass weder Transparenz- noch Kontrollmechanismen eine Eingrenzung sicherstellen. Dadurch ausgelöste Verunsicherung beeinträchtigt die Menschen nicht nur in der Wahrnehmung ihrer Freiheitsrechte, sondern auch deren Vertrauen in die Polizei. Mit der Entgrenzung der polizeilichen Befugnisse wird der PAG-E zum Bärendienst für die Polizei.

Durch die Pflicht, mit dem Polizeirecht die DSRl-JI, also europäisches Recht, umzusetzen, ist das PAG nicht nur am nationalen Verfassungsrecht, sondern auch am **europäischen Recht** und insbesondere an der europäischen Grundrechte-Charta (GRCh) zu messen. Die dadurch vorgegebenen Anforderungen entsprechen weitgehend denen des nationalen Verfassungsrechts, gehen aber teilweise, etwa bei den Diskriminierungsverboten (Art. 21 GRCh) darüber hinaus. Die Anwendbarkeit des Europarechts hat zur Folge, dass Gerichte – sollten sie insofern einen Verstoß erkennen – ein Vorlageverfahren beim Europäischen Gerichtshof initiieren können (Art. 267 AEUV).

Bevor der Bayerische Landtag eine Ausweitung der Befugnisse im Polizeirecht vorsieht, ist er aufgefordert, bezüglich der bestehenden Regelungen Europarechts- und Verfassungskonformität herzustellen. In einem weiteren Schritt könnte über eine Evaluation festgestellt werden, inwieweit durch den Wandel der Gefahren und der technischen Möglichkeiten Ergänzungsbedarfe bestehen. Es steht zur befürchten, dass der Landtag diesem Rat nicht folgen wird. Umso wichtiger ist es, frühzeitig und umfassend die neuen Befugnisse öffentlich zu erörtern. Im aktuellen Gesetzgebungsverfahren bestehen hierfür nicht (mehr) die nötige Zeit und der nötige Rahmen. Problematische Regelungen sollten **so früh wie möglich auf den rechtlichen Prüfstand** gestellt werden. Nur so kann verhindert werden, dass die bayerischen Regelungen zum Vorbild für andere Bundesländer oder gar für den nationalen Gesetzgeber genommen werden.

Quelle: https://dvd-ev.de/GBayPAGE

1 BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, NJW 2016, 1781 = DuD 2016, 469 = EuGRZ 2016, 149 = DVBl 2016, 770 = K&R 2016, 395 = NVwZ 2016, 839 (LS mit Anm. Wiemers) = CR 2016, 796 (BKA-Gesetz).

2 BVerfG 27.02.2008 – 1 BvR 370/07 u. 1 BvR 595/07, NJW 2008, 822 = DÖV 2008, 459 = MMR 2008, 315 = DVBl 2008, 411 (Online-Durchsuchung); Weichert in Däubler u. a., Bundesdatenschutzgesetz, 5. Aufl. 2016, Einl. Rn. 13.

3 Weichert in Däubler u. a. (Fn. 2), Einl. Rn. 30 ff.

4 Dazu kritisch Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD), Stellungnahme vom 21.12.2017, https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf, S. 7 f.; Löffelmann, Stellungnahme zum PAG-Entwurf eines PAG-Neuordnungsgesetzes vom 14.02.2018, Rn. 11.

5 Dazu kritisch BayLfD (Fn. 4), S. 11 f.; Löffelmann (Fn. 4), Rn. 17.

6 Dazu kritisch BayLfD (Fn. 4), S. 15 ff.

7 Dazu kritisch BayLfD (Fn. 4), S. 17 ff.; Löffelmann (Fn. 4), Rn. 24.

8 Dazu kritisch BayLfD (Fn. 4), S. 20 f., 69 f.

9 Dazu kritisch BayLfD (Fn. 4), S.24; Löffelmann (Fn. 4), Rn. 31; Graulich, Gutachterliche Anmerkungen zu den Gesetzentwürfen der Bayerischen Staatsregierung v. 14.03.2018, S. 17 ff.

10 Dazu kritisch BayLfD (Fn. 4), S. 25.

11 Dazu kritisch Löffelmann (Fn. 4) Rn. 35

12 Dazu kritisch BayLfD (Fn. 4), S. 31 f.; Löffelmann (Fn. 4), Rn. 36.

13 Dazu kritisch BayLfD (Fn. 4) S. 32.

14 Dazu kritisch BayLfD (Fn. 4), S. 35; Löffelmann (Fn. 4) Rn. 47, 49.

15 Dazu kritisch BayLfD (Fn. 4), S. 36 ff.; Löffelmann (Fn. 4) Rn. 47.

16 Dazu kritisch BayLfD (Fn. 4) S. 39 f.; Löffelmann (Fn. 4) Rn. 53-56.

17 Dazu kritisch BayLfD (Fn. 4), S. 43 ff.; Löffelmann (Fn. 4) Rn. 74.

18 Dazu kritisch BayLfD (Fn. 4), S. 46 f.; Löffelmann (Fn. 4) Rn. 79 f.

19 Dazu kritisch BayLfD (Fn. 4), S. 50 ff.; Löffelmann (Fn. 4) Rn. 97.

20 Dazu kritisch BayLfD (Fn. 4), S. 55 ff., 66.

21 Dazu kritisch BayLfD (Fn. 4), S. 58 ff., 74 ff.; Löffelmann (Fn. 4) Rn. 119; Wächtler, Stellungnahme zu den Gesetzentwürfen der Staatsregierung für ein Gesetz zur Neuordnung des bayerischen Polizeirechts v. 20.03.2018, S. 7 ff.

22 Dazu kritisch BayLfD (Fn. 4), S. 60 ff.

23 Dazu kritisch BayLfD (Fn. 4), S. 74.

24 Stand 26.03.2018, abzurufen unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2018_baypagudna_final.pdf, S. 12.

25 BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09 (Fn. 1), Rn. 112, NJW 2016, 1785.

26 Kritisch dazu Löffelmann (Fn. 4), Rn. 3-5; Kohnen, 20.03.2017, https://bayrvr.de/2017/03/20/bayerischer-richterverein-stellungnahme-zum-entwurf-eines-gesetzes-zur-effektiveren-ueberwachung-gefaehrlicher-personen/, Nr. 2; Busch, Ein nächster Schritt in Richtung Guantánamo, http://www.grundrechtekomitee.de/node/874, 27.07.2017.

27 BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09 (Fn. 1) Rn. 116, 168; NJW 2016, 1785, 1791.

28 BVerfG 27.02.2008 – 1 BvR 370/07 u. 1 BvR 595/07, NJW 2008, 822 = MMR 2008, 315 = DVBl 2008, 582. (Online-Durchsuchung).

29 BayLfD (Fn. 4), S. 10 f.; Löffelmann (Fn. 4), Rn. 14-16; Graulich (Fn. 9), S. 14 ff.

30 BayLfD (Fn. 4), S. 25; kritisch auch Löffelmann ((Fn. 4) Rn. 32.

31 BVerfG 03.03.2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999 = DVBl 2004, 557 = MMR 2004, 302 (Großer Lauschangriff), insbes. NJW 2004, 1002.

32 Papier in Maunz/Dürig, Grundgesetz, 80. Erg.lfg. Juni 2017, Art. 13 Rn. 107.

33 Nachweise bei BayLfD (Fn. 4), S. 28.

34 Löffelmann (Fn. 4), Rn. 34.

35 Wortgleich Art. 4 Nr. 4 DSGVO, dazu Buchner in Kühling/Buchner, DSGVO 2. Aufl. 2018, Art. 4 Nr. 4 Rn. 5-8.

36 Vgl. Hornung/Schindler ZD 2017, 208.

37 Kritisch zur Eignung Löffelmann (Fn. 4), Rn. 89.

38 BVerfG 23.02.2007 – 1 BvR 2368/06, NVwZ 2007, 690 (Videoüberwachung); BVerfG 11.03.2008 – 1 BvR 2074/05 u. 1 BvR 1254/07, NJW 2008, 1505 = MMR 2008, 308 = DVBl 2008, 575 (Kfz-Kennzeichen); BVerfG 11.03.2009 – 2 BvR 941/08, NJW 2009, 3293 = DVBl 2009, 1237 = DÖV 2009, 866 (Geschwindigkeitskontrolle).

39 Weichert ZD 2012, 503.

40 BVerfG 02.03.2010 – 1 BvR 256/08 u. a., BVerfGE 125, 323 (Vorratsdatenspeicherung).

41 BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, Rn. 130, BVerfGE 141 280 f.

42 BayLfD (Fn. 4), S. 2 f.; Löffelmann (Fn. 4), Rn. 6, 121 f.; Wächtler (Fn. 21), S. 1 ff.

Pressemitteilung des Netzwerks Datenschutzexpertise vom 15.03.2018

In Bayern für die Polizei geplante DNA-Analyse-Befugnisse sind verfassungswidrig



Bild: AdobeStock

Am 30. Januar 2018 legte die Bayerische Staatsregierung den Entwurf einer Neuordnung des bayerischen Polizeirechts vor, der viele verfassungsrechtlich problematische und nicht akzeptable neue polizeiliche Befugnisse vorsieht, u. a. die Identifikation mit Hilfe von Gendaten (DNA) sowie die Ableitung von Augen-, Haar- und Hautfarbe, des sog. biologischen Alters sowie der sog. biogeografischen Herkunft eines Spurenverursachers aus der DNA. Auf Bundesebene haben sich CDU/CSU und SPD im Koalitionsvertrag für die nächste Legislaturperiode verabredet, entsprechende Regelungen zu verabschieden. Mit einem Bundesinnenminister und früheren bayerischen Ministerpräsidenten Horst Seehofer drohen die jetzt geplanten gesetzlichen Vorschläge zum Vorbild für den Bund zu werden.

In einer umfangreichen Stellungnahme weist das Netzwerk Datenschutzexpertise unter Verweis auf die biotechnischen Gegebenheiten und die Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofes darauf hin, dass die geplanten Regelungen verfassungs- und europarechtswidrig sind: Der Entwurf geht von falschen faktischen Voraussetzungen aus. Erlaubt würden ungeeignete und unverhältnismäßige Maßnahmen mit einem hohen Diskriminierungsrisiko, ohne dass Schutzvorkehrungen vorgesehen sind. Zudem fehlt eine Gesetzgebungskompetenz für Bayern.

Thilo Weichert vom Netzwerk Datenschutzexpertise: „Mit einer solchen bayerischen Sicherheitspolitik droht ein Rückfall in Zeiten, in denen verfassungsrechtliche Werte wie der Datenschutz und die Wahrung des allgemeinen Persönlichkeitsrechts beiseite geschoben wurden. Mit der DNA-Phänotypisierung stößt sie zudem die Tür auf für Gruppendiskriminierungen wegen der „biogeografischen Herkunft“ sowie von Menschen mit besonderem Aussehen, etwa mit schwarzen Haaren oder schwarzer Hautfarbe. So durchsichtig diese Politik im Vorfeld der bayerischen Landtagswahlen in ihrer rechtspopulistischen Orientierung ist, so inakzeptabel und gefährlich sind die geplanten Befugnisse für ein diskriminierungsfreies Zusammenleben in unserer Gesellschaft und für das Ansehen der Polizei. Es darf keinen Durchmarsch bayerischer Sicherheitspolitik geben, wir brauchen hier vielmehr eine aufgeklärte, an Fakten und freiheitlichen Werten orientierte Diskussion.“

Quelle: http://www.netzwerk-datenschutzexpertise.de/publikationen

Stellungnahme des Netzwerks Datenschutzexpertise zum Gesetzentwurf der Bayerischen Staatsregierung zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz) v. 30.01.2018 (Bayerischer Landtag LT-Drs. 17/20425, künftig zitiert: PAG-E)

Polizeiliche Erhebung und Verarbeitung bzw. Auswertung von DNA-Daten

Stand: 26.03.2018

1 Gesetzgebungszusammenhang

Der Gesetzentwurf enthält eine Vielzahl von hochproblematischen Regelungen zur Verarbeitung personenbezogener Daten. Anlässe für die Gesetzgebung sind – so die Begründung – europäische Vorgaben in der Richtlinie (EU) 2016/680 zum Datenschutz bei Polizei und Justiz vom 27.04.2016 sowie die Umsetzung befugniseinschränkender Rechtsprechung des Bundesverfassungsgerichts. Tatsächlich werden bei dieser Gelegenheit auch viele neue polizeiliche Befugnisnormen vorgeschlagen zwecks „dem Stand der Technik entsprechender Ergänzung und noch effektiveren Ausgestaltung". Bei diesen neuen Befugnisnormen handelt es sich u. a. um die Möglichkeiten

- zum Einsatz von sog. Body Cams selbst in Wohnungen (Art. 33 Abs. 4 PAG-E),
- zur Verwendung von Mustererkennung für Identifizierungszwecke (Art. 33 Abs. 5 PAG-E),
- zur Durchsuchung von Rechnern bei externen Dienstleistern (Art. 43 PAG-E),
- zur Nutzung von Drohnen zum Zweck der Datenerhebung (Art. 47 PAG-E).

Im Rahmen eines gesetzgeberischen Schnellverfahrens droht ohne öffentliche Diskussion die Einführung von qualitativ schwerwiegenden Eingriffsbefugnissen, die eine Vielzahl von Menschen in sensitiven Bereichen erfasst und polizeilichen Maßnahmen aussetzt. Eine umfassende kritische Stellungnahme zum gesamten Gesetzentwurf erfolgt durch den Bayerischen Landesbeauftragten für den Datenschutz.
https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf

„Pionierfunktion" für Deutschland hat der Entwurf durch die Zulassung von polizeilichen DNA-Untersuchungen (Gen-Analysen) zum Zweck der Gefahrenabwehr (Art. 14 Abs. 3, 32 Abs. 1 S. 2 u. 3 PAG-E, vgl. § 19 Abs. 3 HSOG). Der Entwurf beschränkt sich dabei nicht auf reine Identifizierungszwecke, sondern sieht darüber hinaus die DNA-Phänotypisierung (Forensic DNA-Phenotyping – FDP) vor, die bisher in Deutschland überhaupt nicht zulässig ist, selbst nicht in der Strafprozessordnung (StPO).

Bei der geplanten bayerischen Gesetzgebung zur DNA-Phänotypisierung handelt es sich um Landesrecht, mit dem ein Vorbild für bundesweite Regelungen geschaffen werden soll. Dahin gehende – bisher erfolglose – Initiativen strebten die Bundesländer Baden-Württemberg und Bayern im Jahr 2017 im Bundesrat an (zur Änderung des § 81e StPO, BR-Drs. 117/17 und BR-Drs. 117/1/17).[1] Angesichts des Umstandes, dass der bisherige bayerische Ministerpräsident Horst Seehofer Bundesinnenminister der neuen Bundesregierung von CDU/CSU und SPD ist, sind bei einer erfolgreichen Einführung der DNA-Analyse im bayerischen Polizeirecht umgehend inhaltlich entsprechende Initiativen für das deutsche Bundessicherheitsrecht zu erwarten. Die CDU/CSU und die SPD haben in ihrem Koalitionsvertrag für die Ausweitung von DNA-Analysen vereinbart: „Wir stärken die Sicherheit in Deutschland: ... Ausweitung DNA-Analyse" (S. 16, Z. 589). „Die DNA-Analyse wird im Strafverfahren auf äußerliche Merkmale (Haar, Augen, Hautfarbe) sowie Alter ausgeweitet (§ 81e StPO)." (S. 123, Z. 5802)
https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1

Die vorliegende Stellungnahme konzentriert sich auf diese geplanten Regelungen.

2 Regelungsvorschlag

2.1 DNA-Identifizierung

In Art. 14 BayPAG sind „erkennungsdienstliche Maßnahmen" geregelt. Derartige Maßnahmen sind bisher gemäß Abs. 1 zulässig, wenn Nr. *1 eine nach Art. 13 zulässige Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist, 1a. trotz einer nach Art. 13 getroffenen Maßnahme der Identitätsfeststellung Zweifel über die Person oder die Staatsangehörigkeit bestehen, 2. dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, weil der Betroffene verdächtig ist, eine Tat begangen zu haben, die mit Strafe bedroht ist und wegen der Art und Ausführung der Tat die Gefahr der Wiederholung besteht oder 3. dies erforderlich ist zur Abwehr einer Gefahr oder einer drohenden Gefahr für ein bedeutendes Rechtsgut*.

Art. 13 Abs. 1 PAG regelt die „Identitätsfeststellung" und erlaubt diese u. a. *1. zur Abwehr a) einer Gefahr oder b) einer drohenden Gefahr für ein bedeutendes Rechtsgut*.

Als Art. 14 Abs. 3 PAG-E ist nun geplant:
Die Polizei kann dem Betroffenen zudem Körperzellen entnehmen und diese zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen, wenn dies zur Abwehr einer Gefahr für ein bedeutendes Rechtsgut erforder-

lich ist und andere erkennungsdienstlichen Maßnahmen nicht hinreichend sind; bei der Untersuchung darf eine andere Feststellung als die genannte nicht getroffen werden. Ein körperlicher Eingriff darf dabei nur von einem Arzt vorgenommen werden. Die entnommenen Körperzellen sind unverzüglich nach der Untersuchung zu vernichten, soweit sie nicht nach anderen Rechtsvorschriften aufbewahrt werden dürfen. Eine Maßnahme nach Satz 1 darf nur durch den Richter angeordnet werden, bei Gefahr im Verzug auch durch die in Art. 36 Abs. 4 Satz 2 und 3 genannte Personen.

Eine Begründung für die Notwendigkeit der DNA-Identifizierung zum Zweck der Gefahrenabwehr wird im Entwurf nicht gegeben (S. 41 f.).

2.1 DNA-Phänotypisierung

Der bisherige Art. 31 PAG zur „Datenerhebung" soll zum Art. 32 werden.

In Art. 32 Abs. 1 S. 1 Nr. 1 PAG-E ist vorgesehen, dass es der Polizei erlaubt ist, Daten *über die in Art. 7, 8 und 10 genannten Personen und über andere Personen zu erheben, wenn dies erforderlich ist 1. zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten (Art. 2 Abs. 1)*.

Die Zulassung von DNA-Phänotyp-Untersuchung ist gemäß Art. 32 Abs. 1 S. 2 PAG-E geplant:

Im Fall des Satzes 1 Nr. 1 kann die Datenerhebung durch die molekulargenetische Untersuchung aufgefundenen Spurenmaterials unbekannter Herkunft zum Zwecke der Feststellung des DNA-Identifizierungsmusters, des Geschlechts, der Augen-, Haar- und Hautfarbe, des biologischen Alters und der biogeographischen Herkunft des Spurenverursachers erfolgen, wenn die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Bei der Untersuchung dürfen andere Feststellungen als die in Satz 2 genannten nicht getroffen werden.

Eine konkretisierende Begründung für die Notwendigkeit der DNA-Merkmalszuordnung wird nicht gegeben (S. 50). Es wird u. a. ausgeführt:

Im neuen Abs. 1 Satz 2 erfolgt auf Grund der Relevanz für Maßnahmen der Gefahrenabwehr eine ausdrückliche Regelung für die DNA-Bestimmung von (zunächst) unbekanntem, aufgefundenem Spurenmaterial zu präventiv-polizeilichen Zwecken. […] Gerade weil es sich hier um zunächst unbekannte Personen handelt, darf sich die Feststellung neben dem DNA-Identifizierungsmuster auch auf das Geschlecht, die Augen-, Haar- und Hautfarbe sowie das biologische Alter und die biogeographische Herkunft eines Spurenverursachers beziehen. […] Rückschlüsse auf persönlichkeitsrelevante Merkmale wie Erbanlagen, Charaktereigenschaften oder Krankheiten des Betroffenen, also ein Persönlichkeitsprofil, werden damit nicht ermöglicht.

3 Bewertung allgemein

DNA-Daten unterscheiden sich von sonstigen personenbezogenen Daten durch folgende **persönlichkeitsrechtlich relevante Eigenschaften**:

- Es besteht eine weitgehende Unveränderbarkeit dieser Daten eines Menschen von dessen Zeugung bis weit nach dem Tod.
- Dadurch eignen sich diese Daten als eindeutiger (biometrischer) Identifikator des Menschen.
- Dies führt dazu, dass sowohl der genetische Code als auch die Gewebeproben, aus denen dieser gewonnen wird, nicht wirksam anonymisiert werden können.
- Die DNA-Daten sind somit „schicksalhaft" den jeweiligen Betroffenen vorgegeben und zwar auch in Bezug auf höchstpersönliche Eigenschaften.
- Diese Eigenschaften sind teilweise von höchster Sensibilität, etwa wenn sie sich auf die seelische oder gesundheitliche Disposition beziehen.
- Oft lassen sich insofern aber keine objektiv eindeutigen Aussagen machen; vielmehr sind nur vage Wahrscheinlichkeitsaussagen (Prognosen) möglich.
- Durch die Allgegenwärtigkeit des Trägermaterials, also z. B. von Haaren, Hautschuppen, Speichel, sonstigen Körperflüssigkeiten, können Betroffene weder kontrollieren noch verhindern, dass und wo dieses Material hinterlassen und evtl. von Dritten erfasst und ausgewertet wird.
- Die Erfassung und Auswertung von DNA-Daten ist mit den menschlichen Sinnen nicht möglich, es bedarf eines komplexen technischen, für die Betroffenen intransparenten Verfahrens, das i. d. R. nur Experten zugänglich und nur durch diese überprüfbar ist.
- Schließlich hat der genetische Code nicht nur Aussagekraft bezüglich der betroffenen Person selbst, sondern auch bezüglich der biologischen Verwandten mit einer manchmal hohen und präzise zu bestimmenden statistischen Wahrscheinlichkeit.[2]

Wegen der sich daraus ergebenden Sensitivität hat der europäische Gesetzgeber diese Datenart als **besondere Kategorie personenbezogener Daten** und damit als besonders schutzbedürftig eingestuft (Art. 4 Nr. 13, Art. 9 Verordnung (EU) 2016/679, Europäische Datenschutz-Grundverordnung – DSGVO, Art. 4 Nr. 12, Art. 10 Richtlinie (EU) 2016/680, Europäische Datenschutz-Richtlinie Justiz-Polizei – DSRl-JI: genetische Daten, biometrische Identifikatoren). Zudem handelt es sich bei genetischen Daten um biometrische Identifikatoren (Art. 4 Nr. 14 DSGVO, Art. 4 Nr. 12 DSRl-JI), die ebenso als besondere Datenkategorie zu behandeln sind.[3] Nach Art. 10 DSRl-JI darf eine Verarbeitung solcher Daten erfolgen, *wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und a) wenn sie nach dem Unionsrecht oder dem Rechts der Mitgliedsstaaten zulässig ist, b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder c) wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.*

Die Gesetzesbegründung des PAG-E führt an keiner Stelle auf, weshalb die DNA-Daten erforderlich sind. Es fehlt somit an der gemäß Art. 10 DSRl-JI geforderten **Begründung der Erforderlichkeit**.

Es ist anerkannt, dass DNA-Identifizierungsmuster im Rahmen der Strafverfolgung erforderlich sein können. Analysen können aber grundsätzlich nicht zur **Abwehr von Gefahren** oder auch zum präventiven Einsatz gegen künftige Straftaten, also zur Verhinderung künftiger Straftaten genutzt werden.[4] Die Aufklärung künftiger Straf-

taten ist in § 81g StPO geregelt. Dieses Bundesgesetz hindert eine landesrechtliche Regulierung (Art. 70 GG).[5]

Gemäß der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) und des Europäischen Gerichtshofs (EuGH) sind hoheitliche Maßnahmen, die in das Grundrecht auf informationelle Selbstbestimmung bzw. in das Grundrecht auf Datenschutz eingreifen, „nur im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit" erlaubt. Diese Einschränkung darf nicht weiter gehen, als es **zum Schutze öffentlicher Interessen unerlässlich** ist".[6]

Wegen der Sensitivität der Daten des spezifischen hoheitlichen Eingriffscharakters stellt das BVerfG hohe Anforderungen an den Einsatz polizeilicher Maßnahmen. Im Rahmen strafrechtlicher Ermittlungen ist die genetische Identifikation nur zur Aufklärung von „Straftaten mit erheblicher Bedeutung" zulässig. Das BVerfG untersagt eine pauschale Bewertung und verlangt, dass in jedem Einzelfall eine umfassende Abwägung aller relevanten Aspekte zu erfolgen hat, wozu u. a. die jeweilige Eingriffstiefe der Maßnahme, die Schwere der aufzuklärenden Straftat sowie die Aufklärungswahrscheinlichkeit angesichts der tatsächlichen Umstände gehören. Weiterhin betont das BVerfG hinsichtlich einer Speicherung der Daten das Resozialisierungsinteresse von verurteilten Straftätern. Dieses zwingt dazu, bei der Speicherung der DNA-Daten bestimmte angemessene Tilgungsfristen zu beachten. Hinsichtlich der Anforderungen an die Eingriffsnorm bekräftigt das BVerfG seine allgemeine Rechtsprechung, wonach die gesetzliche Regelung normenklar und justiziabel sein muss.[7]

Art. 10 DSRl-JI fordert bei der Regulierung der Verarbeitung genetischer Daten „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person". Solche Garantien können in materiellrechtlichen Anforderungen, in einem spezifischen Kernbereichsschutz und Diskriminierungsverboten, in Anforderungen an das Verfahren, an Kontrollen, an Standards, an Zertifizierungen oder an Evaluierungen bestehen.[8]

Angesichts des Umstands, dass die reinen Materialkosten pro DNA-Analyse für Identifizierungszwecke äußerst niedrig sind und im Gesetzentwurf mit ca. 25 € angegeben werden (S. 4), besteht die Gefahr, dass diese zu einer **Standardmaßnahme** wird – selbst bei einer rechtlich eingeschränkten Regelung, die den Ausnahmecharakter dieser Maßnahme betont.[9] Diese Einschätzung wird dadurch gestützt, dass die bisher im Strafprozessrecht vorgesehenen Maßnahmen der DNA-Erhebung, -Speicherung und -Nutzung in der Praxis weit über das zugelassene Maß hinaus angewendet werden, so dass die vorhandenen individuellen Rechtsschutzmöglichkeiten nicht genügen, eine weitgehend rechtskonforme Praxis sicherzustellen.[10] Zwar dürften sich die Kosten für die Gutachtenerstellung zur DNA-Phänotypisierung je nach Fragestellung und Methode noch im dreistelligen Eurobereich bewegen, doch ist auch wegen der biotechnologischen Fortschritte künftig eine starke Kostenreduzierung zu erwarten.

4 Genetische Identifizierung

Gemäß dem geplanten § 14 Abs. 3 PAG-E wird eine genetische Identifizierung bei einer Gefahr für ein bedeutendes Rechtsgut erlaubt. Diese Regelung genügt nicht den verfassungsrechtlichen Bestimmtheitserfordernissen. Es wird kein Unterschied gemacht, ob es sich bei dem **Betroffenen** um einen Störer, ein Opfer oder um eine dritte Person (Art. 10 PAG) handelt. Damit wird Art. 6 DSRl-JI missachtet, der eine Differenzierung nach verschiedenen Personengruppen fordert (Straftäter, Verdächtige, Opfer, Zeugen, Hinweisgeber, andere).

Der Begriff des **„bedeutenden Rechtsguts"** ist auch unbestimmt. Den Rechtsanwendenden werden nicht genügend Hinweise für eine begrenzende Auslegung gegeben. Der Begriff bezieht sich auf Art. 11 Abs. 3 S. 2 Nr. 1-3, 5 PAG: *Bedeutende Rechtsgüter sind: 1. der Bestand oder die Sicherheit des Bundes oder eines Landes, 2. Leben, Gesundheit oder Freiheit, 3. die sexuelle Selbstbestimmung, 4. erhebliche Eigentumspositionen oder 5. Sachen, deren Erhalt im besonderen öffentlichen Interesse liegt*. Es genügt also u. a. für die Durchführung einer DNA-Identifikation eine Gefahr für erhebliches Eigentum, wobei unklar bleibt, wo die Erheblichkeitsschwelle anzusetzen ist.

Erst auf Intervention des Bayerischen Landesbeauftragten für Datenschutz (BayLfD) wurde als **Einschränkung** für die Zulässigkeit zur Voraussetzung gemacht, dass „andere erkennungsdienstliche Maßnahmen nicht hinreichend sind", die Maßnahme zur Gefahrenabwehr „erforderlich" sein muss und dass „eine andere Feststellung als die genannte nicht getroffen werden" darf.

Die in § 14 Abs. 3 S. 2 vorgesehene Regelung, dass **körperliche Eingriffe** „nur von einem Arzt durchgeführt werden" dürfen, stellt keine quantitative oder qualitative Beschränkung dieser Maßnahme dar, da – so die Gesetzesbegründung – „die Gewinnung von DNA-Material durch Eindringen in natürliche Körperöffnungen, etwa im Wege eines (Mundhöhlen-)Schleimhautabstrichs, nur eine einfache körperliche Untersuchung und gerade kein körperlicher Eingriff im Sinne dieser Norm" sei (S. 41). Für das Erlangen des Materials genügt also nach Ansicht des Normgebers das einfache Tätigwerden eines Polizeibeamten. Diese Bewertung mit den sich ergebenden Konsequenzen ist fragwürdig: Auch wenn die Probenentnahme per Schleimhautabstrich keine Körperverletzung darstellt, ist damit ein körperlicher Eingriff gegeben, der einen erhöhten Rechtfertigungsbedarf begründet.[11]

Nicht nur die Vornahme der Probenentnahme, sondern auch die Entscheidung hierüber kann „bei **Gefahr im Verzug**" „kraft Delegation auch durch einen Polizeivollzugsbeamten mit der Qualifizierung für Ämter ab der 4. Qualifikationsebene oder Beamte mit der Befähigung zum Richteramt angeordnet" werden (§ 36 Abs. 4 S. 2, 3 PAG-E). Eine richterliche Bestätigung ist erst gemäß Art. 92 Abs. 3 PAG-E binnen drei Tagen nötig (S. 41). Durch diese Regelung wird die verfahrensrechtliche Grundrechtsicherung durch den Richtervorbehalt faktisch ausgehebelt, da von der Ausnahme in Gefahrensituationen regelmäßig Gebrauch gemacht werden wird. Damit ist eine verfassungsrechtlich vorbeugende Kontrolle der Maßnahme durch eine unabhängige neutrale Instanz[12] nicht gewährleistet.


Bild: AdobeStock

Eine Begrenzung der **Speicherdauer** der DNA-Identifizierungsmuster ist nicht vorgesehen; der weitere Umgang hiermit ist nicht geregelt. Zwar schreibt S. 3 der Regelung die unverzügliche Vernichtung der Körperzellen vor. Selbst dies wird eingeschränkt, wenn eine zweckändernde Aufbewahrung, z. B. für Strafverfolgungszwecke (§ 81a Abs. 3 StPO) möglich ist. Zum Umgang mit dem – für das weitere Verfahren relevanten – Untersuchungsergebnis wird nichts ausgeführt. Gemäß Art. 14 Abs. 4 PAG-E ist eine Vernichtung der Unterlagen nur vorgesehen, wenn die materiellrechtlichen Voraussetzungen des Abs. 3 entfallen sind, also wenn sich im Nachhinein herausstellt, dass die Erfassung unzulässig war. Es ist so nicht gewährleistet, dass die Löschung erfolgt, soweit und sobald die Muster nicht (mehr) „unbedingt erforderlich" sind (Art. 10 DSRl-JI).

Das BVerfG fordert für hoheitlich erfasste DNA eine strenge **Zweckbindung**. Hierdurch und durch eine frühzeitige Vernichtung des entnommenen Zellmaterials soll dem Missbrauch, auch der Untersuchung im codierenden Bereich der DNA, vorgebeugt werden.[13] Der Entwurf sieht dem gegenüber ausdrücklich vor, dass die erlangten Informationen weitergenutzt werden können, solange die Voraussetzungen von Art. 14 Abs. 1 oder 3 PAG-E gegeben sind (u. a. „vorbeugende Bekämpfung von Straftaten" sowie „Abwehr einer Gefahr oder einer drohenden Gefahr für ein bedeutendes Rechtsgut"). Es ist daher davon auszugehen, dass die erlangten Identifizierungsmuster in der bundesweiten beim Bundeskriminalamt (BKA) geführten DNA-Analyse-Datei (DAD) gespeichert werden und für weitere polizeiliche Zwecke genutzt werden (§ 81g Abs. 5 StPO). Das BVerfG hat darauf hingewiesen, dass dem Rehabilitationsinteresse von Betroffenen gegenüber der Gefahr sozialer Abstempelung durch Tilgungsfristen entsprochen werden muss.[14] Auch dies steht einer Weiternutzung der Untersuchungsergebnisse entgegen. Das BVerfG hat für eine zweckändernde Weiternutzung von Daten das Kriterium der „hypothetischen Datenneuerhebung" entwickelt. Danach kann eine Zweckänderung zulässig sein, wenn die Daten auch für den neuen Zweck erhoben werden dürften.[15]

Die im Entwurf erlaubte **zweckändernde Nutzung** geht über die in Abs. 3 geregelten Erhebungsvoraussetzungen hinaus, indem keine „erhebliche Straftat" (§ 81g Abs. 1 StPO) gefordert wird und gar eine Nutzung im Vorfeld einer Gefahr („drohende Gefahr") erlaubt wird. Diese weitgehenden Aufbewahrungsregeln stehen im eindeutigen Widerspruch zur bisherigen Verfassungsrechtsprechung.[16]

Der Entwurf enthält keine in Art. 10 DSRl-JI geforderten angemessenen **geeigneten Garantien**. So ist z. B. keine Übermittlungsbegrenzung vorgesehen (vgl. § 81g Abs. 5 S. 3 StPO). Auch eine Unterrichtungspflicht bei verdeckten Maßnahmen fehlt (vgl. § 19 Abs. 5 S. 2 HSOG). Dies führt zur Unverhältnismäßigkeit der Befugnis und zur Europarechtswidrigkeit der Verwendungsregelungen.

5 DNA-Phänotypisierung

In der Gesetzesbegründung wird in Frage gestellt, ob einer DNA-Analyse „von (zunächst) unbekanntem, aufgefundenem Spurenmaterial zu präventiv-polizeilichen Zwecken" überhaupt **Rechtseingriffscharakter** zukommt, so dass es hierfür einer Befugnisnorm bedarf. Dabei wird auf den PAG-Kommentar von Schmidbauer/Steiner verwiesen.[17] Deren Ansicht ist sehr streitig



und wird, soweit erkennbar, nur von den zitierten Autoren vertreten. Für die Annahme eines informationellen Eingriffs kommt es nicht darauf an, dass eine Person schon namentlich bekannt ist. Es genügt, dass eine Person bestimmbar ist.[18] Die Bestimmbarkeit ist gerade Sinn und Zweck dieser DNA-Analyse.

Die Gesetzesbegründung zur DNA-Phänotypisierung nimmt selbst keine verfassungsrechtliche Bewertung vor, sondern verweist „zur verfassungsrechtlichen Zulässigkeit dieser Feststellungen" auf „die BR-Drs. 117/17 und den zugehörigen Plenarantrag BR-Drs. 117/1/17, der wiederum auf BVerfGE 103, 21 Bezug nimmt"[19] (S. 50).

Begründet wird BR-Drs. 117/17 wie folgt: „Diese äußerlich sichtbaren Körpermerkmale (Augenfarbe, Haarfarbe, Hautfarbe sowie biologisches Alter) können nach den **wissenschaftlichen Erkenntnissen** durch Untersuchungen genetischer Informationen mit der im Folgenden jeweils angegebenen Vorhersagegenauigkeit bestimmt werden: Augenfarbe blau oder braun: 90-95%, Haarfarben rot, blond, braun oder schwarz: 75-90%, Hautfarbe: helle und dunkle Hauttypen: 98%. [...] Die Vorhersagegenauigkeit in Bezug auf das biologische Alter einer Person liegt bei +/- 3 bis 5 Jahren. Im Einzelfall sind Abweichungen bis zu zehn Jahren möglich." In BR-Drs. 117/1/17 heißt es ergänzend: „Nach Auskunft der Gemeinsamen Kommission der rechtsmedizinischen und kriminaltechnischen Institute liegen darüber hinaus aussagekräftige DNA-Tests vor, die ermöglichen, aus kleinsten DNA-Mengen die kontinentale Herkunft einer Person mit einer Wahrscheinlichkeit von über 99,9 Prozent zu bestimmen".

Gemäß den zitierten Bundesratsanträgen bestünden keine verfassungsrechtlichen Bedenken gegen die geplante Ausweitung der Untersuchungsmöglichkeiten. Der Kernbereich der Persönlichkeit sei nicht betroffen. Die Merkmale seien ja äußerlich ohnehin erkennbar. Bei der Prüfung, ob in den verfassungsrechtlich **absolut geschützten Kernbereich** der Persönlichkeit eingegriffen wird, hat das BVerfG bzgl. der DNA-Identifizierungsmuster in der in der Entwurfsbegründung zitierten Entscheidung darauf abgestellt, dass keine „Rückschlüsse auf persönlichkeitsrelevante Merkmale wie Erbanlagen, Charaktereigenschaften oder Krankheiten, also ein Persönlichkeitsprofil" gezogen werden können.[20] Genau auf solche Erbanlagen soll aber hier geschlossen werden.

Die Haarfarbe ist oft vom Alter abhängig. Es ist zumindest fragwürdig, die Augenfarbe und das „biologische Alter" als **„äußerlich sichtbare Merkmale"** zu bezeichnen. Ebenso wenig kann davon bei der „kontinentalen Herkunft" die Rede sein.

Von der Politik und der Polizeipraxis werden völlig **überzogene Erwartungen** an die Aussagekraft der DNA-Analyse geweckt. So setzte der baden-württembergische Justizminister Guido Wolf die Bestimmung äußerer Merkmale per DNA mit der Verwertung einer Videoaufzeichnung gleich.[21] Nordrhein-Westfalens Innenminister Herbert Reul beklagte, dass Beschlüsse der Innenministerkonferenz zur erweiterten Nutzung von DNA-Analysen nicht konsequent umgesetzt würden: „Es versteht kein Mensch, dass Forensiker heute aus winzigen Spuren sehr präzise genetische Phantombilder erstellen können, die unsere Polizisten jedoch nicht nutzen dürfen."[22] Der Leiter des baden-württembergischen Landeskriminalamtes Ralf Michelfelder erklärte: „Die DNA ist ein stummer Zeuge – ein Zeuge wie jeder andere auch. Wir wollen nicht mehr sehen als das, was ein anderer Zeuge sehen und berichten kann".[23] Selbst in polizeilichen Publikationen mit wissenschaftlichem Anspruch ist – absolut realitätsfern – vom „genetischen Phantombild" die Rede.[24] Zugleich wird selbst von polizeilichen DNA-Analytikern wie z. B. Harald Schneider vom Landeskriminalamt Wiesbaden zugestanden, dass zur sog. biogeografischen Herkunft, zu Gesichtsform oder Body-Mass-Index oder zu Dispositionen für Erbkrankheiten eines Spurenlegers voraussichtlich erst in etwa 5 Jahren Aussagen gemacht werden können.[25]

Die Feststellung des **Geschlechts** ist durch die Untersuchung nicht-codierender DNA-Sequenzen möglich. Etwas anderes gilt für die weiter vorgesehenen Merkmale (Augen-, Haar- und Hautfarbe, biologisches Alter, „biogeographische Herkunft")

Der Gesetzentwurf geht von **falschen Fakten** aus. Die angegebenen Prognosesicherheiten sind falsch bzw. teilweise grob verzerrend. Er stützt sich hinsichtlich der wissenschaftlichen Grundlagen der DNA-Analysen auf den bayerischen Antrag im Bundesrat zur Reform des § 81e StPO und damit auf die Wahrscheinlichkeitsangaben, die bereits ein Jahr umfassend kritisiert wurde[26]:

Die angegebenen Prognosesicherheiten sind nicht die für den Ermittlungsfall relevanten **Wahrscheinlichkeiten und irreführend hoch**. Die genauen Vorhersagewahrscheinlichkeiten sind Gegenstand der aktuellen Forschung und können je nach untersuchter Gruppe und untersuchter Eigenschaft deutlich schwanken. Die erzielbaren Wahrscheinlichkeitsaussagen werden sich auf einem niedrigeren Niveau bewegen. Sie sind abhängig von der untersuchten Gruppe, der Referenzgruppe sowie von der verwendeten Methode. [27] Dies hat zur Folge, dass keine pauschalen forensischen Wahrscheinlichkeitsaussagen gemacht werden können, diese vielmehr für jede Einzeluntersuchung und für jedes Merkmal unter Bezugnahme auf das angewandte Modell und die verfügbaren Referenzdaten getroffen werden müssen.

Einzig für die **Augenfarbe** gibt es weiterführende Analysen, die die ermittlungsrelevanten Wahrscheinlichkeiten anführen.[28] So kann die Vorhersageswahrscheinlichkeit für braune Augen in Populationen, in denen diese selten sind, auf 65% sinken. Weil die Vorhersage für seltene Merkmale ungenauer werden kann, aber genau in diesen Fällen für die Fokussierung auf eine kleinere Gruppe besonders nützlich zu sein scheint, ergibt sich bei der Methode der phänotypisierenden DNA-Analyse systembedingt ein doppeltes Diskriminierungsrisiko in Bezug auf Personengruppen mit seltenen Merkmalen.

Aus wissenschaftlicher Sicht ist insbesondere die angebliche Genauigkeit von 99.9.%, mit der die „**biogeografischen Herkunft**" (engl. "biogeographical ancestry", im Folgenden: BGA) in einer Ermittlung abgeleitet werden kann, äußerst spekulativ. Die Analyse lässt nur sehr bedingt Rückschlüsse auf die tatsächliche Herkunft einer Person zu. Die Ergebnisse hängen davon ab, welche Referenzdatenbank für eine Untersuchung herangezogen wird. Die gegenwärtig von deutschen Forensikern benutzten Referenzdatenbanken sind auf (vermeintlich) „reine Bevölkerungsgruppen" (pure ancestry populations) ausgerichtet und verwenden in erster Linie Y-chromosomale oder mitochondriale Marker. Diese beschreiben entweder die väterliche oder mütterliche Abstammung und sind daher nicht geeignet, die Komplexität von Migration, multiethnischen Gesellschaften und Sexualbeziehungen zwischen Menschen mit unterschiedlicher Herkunft adäquat widerzuspiegeln. Nähere Angaben zur Bestimmungsmethode enthält der Entwurf aber nicht. Bei BGA handelt es sich außerdem nicht – wie behauptet wird – um ein äußerlich erkennbares Merkmal. Diese Behauptung geht von der nicht nur fehleranfälligen, sondern vorurteilsbelasteten Annahme aus, dass „biogeografische Herkunft" „Ethnizität" sei und mit definierten äußeren Merkmalen in Verbindung gebracht werden könne.

Es ist außerdem zu berücksichtigen, dass in den bisherigen Studien mit hochqualitativem Versuchsmaterial und **nicht mit Spurenmaterial** gearbeitet wurde. Wie hoch die Vorhersagewahrscheinlichkeiten für die verschiedenen Merkmale angesichts von DNA-Degradierung oder Kontaminationen durch die DNA Dritter wäre, ist bisher unzureichend untersucht. Es ist jedoch anzunehmen, dass diese niedriger ausfallen oder dass, bedingt durch mangelhafte Spurenqualität, eine Vielzahl an Spuren nicht für die weiterführende DNA-Analyse zugelassen werden dürfte.[29]

Die **Geeignetheit der Maßnahme** wird dadurch weiter reduziert, dass äußere Merkmale gezielt manipuliert werden können (z. B. Färben von Haaren, farbige Kontaktlinsen). Wenn eine Eignung für die Ermittlung besteht, dann zumeist nur ermittlungsintern. Die öffentliche Kommunikation genetisch abgeleiteter wahrscheinlicher Tätermerkmale zu Fahndungszwecken birgt die Gefahr falscher Hinweise und damit der Fehlausrichtung von Hinweisen sowie die Gefahr einer gesellschaftlichen Diskriminierung von seltenen Merkmalsträgern. Hinsichtlich der biogeografischen Herkunft besteht ein besonders hohes Diskriminierungsrisiko (s. u.).

Die Gesetzesbegründungen beschränken sich auf die – inhaltlich nicht näher erläuterte – Behauptung, der **Kernbereich privater Lebensgestaltung** werde nicht tangiert. Tatsächlich sind die Grenzen des unantastbaren Kernbereichs im Bereich der Genanalyse noch nicht ansatzweise wissenschaftlich erörtert, geschweige denn durch die höchstrichterliche Rechtsprechung präzisiert. Der Schutz einer unantastbaren persönlichen Sphäre hängt von bestehenden gesellschaftlichen Werten sowie von technischen Möglichkeiten ab. Dabei müssen die Perspektiven der sich rasant entwickelnden biotechnologischen Erkenntnismöglichkeiten einbezogen werden.

Nach dem Entwurf zulässige Merkmalsangaben sind teilweise höchst aussagekräftig für andere hoch **diskriminierungsträchtige oder hoch sensitive Merkmale**. So sind die Brustkrebsgene BRCA1 und BRCA2 sowie die Blutgerinnungskrankheit des Faktor-XI-Mangels in der aschkenasisch-jüdischen Bevölkerung weit verbreitet, in einem erheblich geringeren Maß bei Menschen mit einem anderen ethnischen Hintergrund.[30] Aus der genetischen Ableitung von äußerlich erkennbaren Merkmalen sind in vielen Fällen Schlüsse auf gesundheitliche und charakterliche Dispositionen möglich. Bei derartigen Rückschlüssen kann schnell der unantastbare Persönlichkeitsbereich tangiert sein. Vorkehrungen gegen solche Rückschlüsse enthält der Entwurf nicht. Aus Äußerungen von Polizeivertretern ist erkennbar, dass in Zukunft selbst Rückschlüsse auf die Disposition für Erbkrankheiten gesetzlich erlaubt werden sollen.[31]

Der Entwurf ignoriert, dass außerhalb des Kernbereichsschutzes eine verfassungsrechtliche **Verhältnismäßigkeitsprüfung** notwendig ist. Er zeichnet sich dadurch aus, dass er sämtliche europa- und verfassungsrechtlichen Anforderungen an qualifizierte Grundrechtseingriffe ausblendet. So wird entgegen der Rechtsprechung des BVerfG keine Begrenzung auf Straftaten mit einer bestimmten Bedeutung, etwa auf die Aufklärung „schwerer Straftaten" vorgenommen. Verfahrensrechtliche Vorkehrungen sind nicht vorgesehen. Auch sonstige Abwägungsparameter werden weder gesetzlich noch in der Begründung eingeführt. Den Anforderungen des Art. 10 DSRl-JI wird damit nicht genügt.

Die **Eignung** der aus DNA abgeleiteten Wahrscheinlichkeitsaussagen zu bestimmten Merkmalen für die Gefahrenabwehr ist nicht im Ansatz dargelegt. Bei einer konkreten Gefahr ist schnelles Handeln notwendig. Eine DNA-Phänotyp-Analyse setzt gegenüber der reinen DNA-Identifizierung eine technisch erheblich aufwändigere Auswertung voraus, was einen Einsatz in Gefahrensituationen typischerweise ausschließt.

Erfolgen Öffentlichkeitsfahndungen auf Grundlage von aus DNA abgeleiteten Merkmalen, so droht nicht nur eine Fehlleitung der Fahndung, sondern regelmäßig auch eine **Diskriminierung** der mit diesen Merkmalen beschriebenen Bevölkerungskreise. Bei einer weißen Hautfarbe ist der Erkenntniswert in Mitteleuropa äußerst gering. Bei einer anderen Hautfarbe besteht dagegen die große Gefahr, dass eine Vielzahl von Personen in polizeiliche Maßnahmen oder Verdächtigungen einbezogen werden, die mit der Gefahrenlage in keinerlei Zusammenhang stehen.[32] Die Art. 3 Abs. 3 GG und Art. 21 Abs. 1 GRCh verbieten die Diskriminie-

rung wegen der Rasse, der Hautfarbe, der ethnischen Herkunft oder der genetischen Merkmale. Die bisher gemachten Erfahrungen mit der Nutzung des „ethnic profiling“ zeigen, dass sowohl bei polizeiinternen Ermittlungen, insbesondere aber bei Öffentlichkeitsfahndungen, große diskriminierende Effekte entstanden.[33] Der Entwurf enthält keine Vorkehrungen, mit denen diese Effekte verhindert oder zumindest reduziert würden. Eine solche könnte darin bestehen, dass erlangte Analyseergebnisse nicht zum Gegenstand öffentlicher Fahndung gemacht werden dürfen.

In Art. 32 Abs. 1 S. 2, 3 PAG-E fehlen Regelungen zur **Speicherungsdauer und zur Verwendung**. Auch insofern ist ein Verstoß gegen Art. 10 DSRl-JI gegeben.

6 Ergebnis

Die geplanten Regelungen zur DNA-Analyse im bayerischen PAG verstoßen gegen deutsches und europäisches Verfassungsrecht sowie gegen die europäischen Vorgaben der DSRl-JI. Erlaubt würden dadurch nicht erforderliche und unverhältnismäßige Maßnahmen mit einem hohen Diskriminierungsrisiko, ohne dass Schutzvorkehrungen vorgesehen sind. Es fehlt an der Gesetzgebungskompetenz des Landes. Die Gefahr der Regelungen besteht nicht nur darin, dass sie unter Verletzung von Grundrechten in Bayern angewendet werden, sondern auch in ihrer beabsichtigten Vorbildwirkung für die Bundesgesetzgebung.

1 Dazu Wienroth/Lipphardt, Wissenschaftliche, ethische & soziale Gesichtspunkte der Anwendung neuer Gen-Analysen im polizeilichen Ermittlungsdienst, BMJV-Symposium 21.03.2017, https://stsfreiburg.files.wordpress.com/2017/05/berlin_vortrag_ausgearbeitet_final-2-mit-aktuellem.pdf.

2 Weichert in Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 13 Rn. 5; Artikel 29 Datenschutzgruppe, Working Paper 91 v. 17.04.2004, S. 5.

3 Weichert in Kühling/Buchner (Fn. 2) Art. 4 Nr. 14 Rn. 3.

4 BVerfG B. v. 14.12.2000 – 2 BvR 1741/99, Rn. 46, , DVBl. 2001, 454; Wollweber NJW 2001, 2304; Sokol in Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006, S. 323 m. w. N.

5 BVerfG U. v. 27.07.2005 – 1 BvR 668/04, Rn. 107, NJW 2005, 2603, 2606; kritisch dazu Schmidbauer/Steiner, Bayerisches Polizeiaufgabengesetz, 4. Aufl. 2014, Art. 11 Rn. 188.

6 BVerfG B. v. 02.07.2013 – 2 BvR 2392/12, Rn. 10; BVerfG B. v. 15.03.2001 – 2 BvR 1841 u. a., NJW 2001, 2321; BVerfG B. 14.12.2000 – 2 BvR 1741/99, Rn. 49, jeweils mit Verweis auf BVerfG U. v. 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419, 422; EuGH U. v. 08.04.2014 – C-293/12, C-594/12, Rn. 38, NJW 2014, 2171.

7 BVerfG, B. v. 14.12.2000 – 2 BvR 1741/99, NJW 2001, 879; BVerfG B. v. 13.03.2001 – 2 BvR 1841/00 u. a., NJW 2001, 2320.

8 Weichert, Genetische Forensik und Datenschutz, Vorgänge Nr. 218 (2/2017), S. 133; Wienroth in Wienroth/Lipphardt (Fn. 1) S. 13 ff.

9 Zu früheren Bestrebungen, die DNA-Analyse zur Standardmaßnahme zu machen, Sokol (Fn. 4) S. 292 f.

10 Beispiele bei Sokol (Fn. 4) S. 303, Petri in Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, A Rn. 127; BT-Drs. 18/13411 zitiert u. a. den baden-württembergischen Datenschutzbeauftragten, S. 2.

11 Kingreen/Poscher in Pieroth/Schlink/Kniesel (Begr.), Polizei- und Ordnungsrecht, 9. Aufl. 2016, S. 238.

12 BVerfG U. v. 12.03.2003 – 1 BvR 330/96 u. 348/99, Rn. 132, NJW 2003, 1795; Sokol (Fn. 4) S. 311; Bosch in Kleinknecht/Müller/Reitberger, StPO-Kommentar, Stand 10/2002 § 81c Rn. 10.

13 BVerfG 14.12.2000 (Fn. 4) Rn. 55; inzwischen ist die Differenzierung zwischen codierenden und nicht-codierenden Bereichen wissenschaftlich überholt, Beck, Forensic DNA-Phenotyping – Bestimmung äußerer Merkmale aus der DNA, KriPoZ 2017, 165; vgl. schon Sokol (Fn. 4) S. 294 f.

14 BVerfG 14.12.2000 (Fn. 4) Rn. 54.

15 BVerfG 20.04.2016 – 1 BvR 966/09, 1140/09, Rn. 287-292, NJW 2016, 1801 f. m. w. N.

16 BVerfG B. v. 02.07.2013 – 2 BvR 2392/12 Rn. 11 m. w. N.

17 Schmidbauer/Steiner (Fn. 5) Rn. 195 ff.

18 Brink in Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, Syst. C Rn. 85; EuGH U. v. 19.10.2016 – C-582/14, Rn. 49, NJW 2016, 3581; auf dieser Erwägung basiert § 81e Abs. 2 StPO.

19 BVerfGE 103, 21 = BVerfG B. v. 14.12.2000 – 2 BvR 1741/99, NJW 2001, 879, DVBl. 2001, 454 (Fn. 4).

20 BVerfG B. v. 14.12.2000 (Fn. 4) Rn. 48

21 Wolf, Ausweitung der DNA-Analyse? NJW-aktuell 3/2017, 16.

22 Jamaika: NRW-Innenminister Reul fordert Sicherheitspaket, www.presseportal.de 18.10.2017.

23 LKA-Chef für Ausweitung von DNA-Analysen, www.zeit.de 09.12.2016.

24 Bundeskriminalamt, Genetisches Phantombild, Stand 12.01.2017; kritisch hierzu Peter Schneider in Genetisches Phantombild per DNA-Analyse? www1.wdr.de 13.06.2017, der die Behauptung, virtuelle Gesichtsbilder aufgrund von DNA-Spuren erstellen zu können, als „eine Schande für die seriöse Wissenschaft“ bezeichnet..

25 Pflüger-Scherb, Interview mit Dr. Harald Schneider über die Entwicklung der DNA-Analyse, www.hna.de 27.10.2017.

26 Lipphardt in Wienroth/Lipphart (Fn. 1) S. 6 ff.

27 Caliebe/Krawczak/Kayser, Predictive values in Forensic DNA Phenotyping are not necessarily prevalance-dependent, Forensic Science International: Genetics, 2017; dazu Buchanan u. a., http://www.fsigenetics.com/article/S1872-4973(18)30035-8/pdf.

28 Caliebe/Krawczak/Kayser (Fn. 27).

29 Uni Freiburg, Droht ein „Alles-ist-erlaubt-Gesetz“? www.pr.uni-freiburg.de 21.03.2018 mit Stellungnahme auf stsfreiburg.wordpress.com/.

30 genomeweb 07.03.2018, 23andMe´s Test OK´d.; Eisner, A New Lens On My Jewishness, In The Form Of A Genetic Disease, forward.com 18.03.2018.

31 Pflüger-Scherb, Interview mit Dr. Harald Schneider über die Entwicklung der DNA-Analyse, www.hna.de 27.10.2017.

32 Schultz/Bartram, Bürgerrechte&Polizei/CILIP 113 (September 2017) S. 73 f.; siehe die Fallbeispiele vom Lipphardt in Wienroth/Lipphardt (Fn. 1) S. 4 f.

33 STS@Freiburg, Offener Brief 08.12.2016, S. 3 ff.; Schultz/Bartram (Fn. 32) S. 74 f.; Gen-ethisches Netzwerk, Stellungnahme: Gegen die Erweiterung polizeilicher Befugnisse in der DNA-Analyse, 25.04.2017, S. 2 f.

Freiheitsfoo

Geleakt: Der Entwurf des neuen Polizeigesetzes für Niedersachsen – Die Polizei auf dem Weg von der Strafverfolgungsbehörde zum präventiven Verfolgungs- und Repressionsapparat für „Gedankenverbrecher"

Nachdem die vorherige rot-grüne Landesregierung Niedersachsens aus eigentümlichen Gründen vorzeitig die Stimmenmehrheit im Landtag verlor und deswegen ihr (nicht unumstrittenes) neues Polizeigesetz nicht installieren konnte, plant die neue rot-schwarze Niedersachsen-GroKo im Sauseschritt ihr eigenes neues Polizeigesetz.

Wie üblich (unabhängig von den regierungsbeteiligten Parteien) passiert das in Niedersachsen ohne Öffentlichkeit und ohne kritische Debatte hinter verschlossenen Türen, im Geheimen. Wer beispielsweise in der beispiellos unübersichtlichen wie bedienerunfreundlichen Homepage des Landtags nach Informationen zum Stand der Dinge suchte, der fand bisher genau Null Verweise zum Vorgang.

Der Entwurf des SPD-CDU-Polizeigesetzes (Niedersächsisches Polizeigesetz – NPOG) mit Stand 19.01.2018 wird in einer übersichtlichen Synopse dem bestehenden „**Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (NdsSOG)" gegenübergestellt und dokumentiert unter:**
https://wiki.freiheitsfoo.de/uploads/Main/Synopse-NdsSOG-NPOG.pdf

Der Entwurf ist vermutlich der mehr oder weniger endgültige Entwurf dieses Gesetzes, zu dem derzeit (ebenfalls intransparent und ohne Aufklärung der Öffentlichkeit) nur noch die Stellungnahmen der Polizei-Lobby-Gruppen eingeholt werden, bevor er in die Landtags-Öffentlichkeit getragen wird, um dann im Innenausschuss behandelt zu werden.

Unserer Erfahrung nach handelt es sich dann allerdings im Wesentlichen nur noch um eine Scheindiskussion, deren Ausgang von vornherein klar scheint. Zumindest wurden in anderen vergleichbaren Fällen die im Zusammenhang einer Innenausschuss-Anhörung zu einem Gesetzentwurf eingeholten Stellungnahmen im Falle von kritischen Inhalten weitgehend ignoriert – es handelt sich bei dem Schauspiel also um einen praktisch als scheindemokratisch zu bezeichnenden Vorgang.


Bild: AdobeStock

Das künftige Gesetz wurde von CDU und SPD durchaus zutreffend auf den Namen „Niedersächsisches Polizeigesetz" (NPOG) getauft, dient es doch vor allem der Ausweitung polizeilicher Befugnisse ins Abstrakte und öffnet ihrer mutmassenden Verdachtsschöpfung Tür und Tor, während der vorherige rot-grüne Entwurf immerhin noch den formellen Anspruch gehabt hat, ein Gefahrenabwehrgesetz zu sein – der „inhaltlich entbehrliche Rechtsbegriff" der „öffentlichen Ordnung" sollte ganz gestrichen werden.

Man konnte mit dem alten rot-grünen Entwurf unter Ausblendung anderer Details also sogar einige wenige positive Tendenzen abgewinnen: So sollten etwa unter dem Stichwort „Racial Profiling" die Strukturen polizeilicher Verdachtsschöpfung verändert werden, in dem die Befugnisse zur verdachtsfreien Kontrolle weitestgehend beschränkt und vor allem der individuellen Entscheidung einzelner PolizistInnen entzogen werden.

Doch schon unter Rot-Grün wurde dieses laut Koalitionsvertrag explizit als zentral ausgewiesene Politikvorhaben von der Polizeiadministration und den Polizeigewerkschaften so lange verschleppt und sturmreif geschossen, bis vom Stärken der Bürgerrechte am Ende nicht mehr viel übrig geblieben war. Der zuletzt diskutierte (und nicht mehr umgesetzte) Entwurf dehnte die Befugnisse der Polizei weit aus und veränderte den Rechtscharakter des Gesetzes sogar grundlegend hin zu einem Tatbestandsrecht. Das Gesetz regelte nämlich plötzlich nicht mehr nur polizeiliche Befugnisse zur Gefahrenabwehr, sondern schuf die Voraussetzung, deren

Durchsetzung über Zwang und Gewaltanwendung hinaus auch noch mit empfindlichen Geldbußen zu verfolgen.

Das damit zwischenzeitlich eingetretene Desaster im ursprünglichen rot-grünen Politikvorhaben treibt nun die Niedersachsen-GroKo auf die Spitze: **Das neue Polizeigesetz wird künftig etwa Verstöße gegen Meldeauflagen der Polizei sogar als Straftaten verfolgbar machen. Und dabei werden die Möglichkeiten der Polizei zum „Predictive Policing" in Form vorbeugender Freiheitsbeschränkungen oder so genannter Gefährderansprachen faktisch enorm ausgeweitet.**

Künftig werden etwa auf so genannte Lagebilder gestützte Mutmaßungen der Polizei für weitreichende Grundrechtseingriffe ausreichen. Die Eingriffsschwelle formuliert der NPOG-Entwurf wie folgt:

„Rechtfertigen bestimmte Tatsachen die Annahme, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat begehen wird, ..."

Schwammiger kann man der Polizei weitreichende Befugnisse wohl kaum mehr zugestehen. Polizeiarbeit soll offenbar immer weniger im Konkreten und immer mehr im Abstrakten rühren. Der Fokus möglicher Sanktionen verschiebt sich von wirklichen Vorfällen auf pure Möglichkeiten.

Das niedersächsische Innenministerium hat, vertreten durch die Polizeidirektion Hannover, im Zuge zweier beim Oberverwaltungsgericht (OVG) Lüneburg anhängiger Verfahren mit Bezug auf das NdsSOG, bei denen es um polizeiliche Videoüberwachung öffentlichen Raums und um die Rechtmäßigkeit der Speicherung personenbezogener Daten von unschuldigen Menschen im Polizeisystem NIVADIS geht, erklärt, dass der Entwurf noch im Jahr 2018 Gesetzeskraft erlangen soll. Diese Verfahren laufen schon seit vielen Jahren, zum Teil seit 2011. Mit dem neuen Gesetz würden zuvor vom Verwaltungsgericht (VG) Hannover als rechtswidrig bewertete Handlungen der Polizei Hannover im Nachhinein legitimiert. Das OVG scheint in beiden Fällen gerne die Verabschiedung des neuen Gesetzes abwarten zu wollen.

Mögen die seit Jahren ständig wiederholten und manches Mal verunglückten Vergleichsversuche mit George Orwells dystopischem Roman „1984" auch nerven und an Kraft verloren haben: Die in diesem Roman geschilderte „Gedankenpolizei", mit der Verfolgung und Unterdrückung von Menschen beschäftigt, die „Gedankenverbrechen" begehen, würde mit dem neuen Polizeigesetz für Niedersachsen ein Stück mehr zur Realität.

Widerstand gegen diese Entwicklungen tut Not.

Der Gesetzentwurf enthält zahlreiche weitere bedenkliche Inhalte, die im Ansatz bereits im Koalitionsvertrag aus dem November 2017 angeklungen sind. Es sei lediglich der irre Passus aus dem „Grundsatz-Kapitel Inneres" des rot schwarzen Koalitionsvertrags (S. 35) zitiert: **„Alle Menschen müssen sich zu jeder Zeit an jedem Ort sicher fühlen."**

Dieser totalitäre, sich selbst kommentierende Anspruch bezeichnet die Denke und das Lebensgefühl der für diesen Passus Verantwortlichen vortrefflich.

Quelle:
https://freiheitsfoo.de/2018/01/30/npog-entwurf/

„Rise of the Police" nun auch in NRW – Eine Zusammenfassung und Kommentierung des geplanten neuen Polizeigesetzes für Nordrhein-Westfalen

Nicht nur in Niedersachsen, auch in anderen Bundesländern sprießen die Gesetze wie Kresse aus dem Boden, die Polizeien und Geheimdiensten bislang unbekannt mächtige Befugnisse, Entscheidungsfreiräume und technische wie rechtliche Möglichkeiten zur ausgeweiteten Überwachung und Repression von nur möglicherweise gefährlich erscheinenden, aber faktisch völlig unschuldigen Menschen („Gedankenverbrechern") zuschustern.

Das jüngste Beispiel hierfür ist der Referentenentwurf eines neuen Polizeigesetzes für Nordrhein-Westfalen (NRW) vom 22.02.2018. *Im Folgenden erfolgt eine sicherlich nicht alle kritischen Punkte betreffende Zusammenfassung und Kommentierung dessen, was sich die schwarz-gelbe Landesregierung in Düsseldorf als neue rechtliche wie technische Gadgets für deren Landespolizei ausgedacht hat. Ähnlich wie die „Grünen" in anderen Landesregierungen entfernen sich hier die „Liberalen" schnellstens von ihren hehren, angeblich freiheitsfreundlichen Idealen, sobald sie in Regierungsverantwortung eingetreten sind.*

Die NRW-Landesregierung will das Polizeigesetz NRW ändern und hat einen Referentenentwurf „Sicherheitspaket I" vorgelegt. Im Zentrum steht das Vorgehen gegen terroristische Bedrohung, aber auch gegen „sonstiges extremistisches Spektrum". Der Referentenentwurf sieht im Wesentlichen folgende Regelungen vor:

1. Einführung des Begriffs der sogenannten **„drohenden Gefahr"** und „drohenden terroristischen Gefahr" als zusätzliche Gefahrenbegriffskategorien nach den Maßgaben des Bundesverfassungsgerichts. Darunter fällt auch die Einführung des Begriffs der drohenden Gefahr „wenn lediglich das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass die Person innerhalb eines absehbaren Zeitraumes eine Straftat von erheblicher Be-

deutung begehen wird" (Änderungen in § 8 Abs. 4, 5 PolG NRW – E)

Problematisch daran ist vor allem, dass diese Begriffsbestimmung dazu genutzt wird, Freiheitsrechte in extremen Maße einzuschränken bei gleichzeitig sehr schwachen Voraussetzungen. Mit den individuellen Verhalten kann auch eine politische Betätigung gemeint sein, sei es das Lesen einer islamistischen Propaganda-Seite oder die Beteiligung an Demonstrationen gegen G20, nach denen es Krawalle gab – wenn mensch polizeiliche Gefahrenprognose liest, ist zu sehen, dass das nicht weit hergeholt ist. Damit ist der Unterdrückung von Oppositionellen Tür und Tor geöffnet.

2. Einführung einer Rechtsgrundlage zur Durchführung von sog. **„Strategischen Fahndungen"** als anlassbezogene, aber verdachtsunabhängige Anhalte- und Sichtkontrollen im öffentlichen Verkehrsraum (Änderungen in § 12a PolG NRW – E)

Praktisch bedeutet dies: Anhalte- und Sichtkontrollen, Schleierfahndung und Gefahrengebiet. Es ist möglich Personen anzuhalten, ihre Identität festzustellen und ihre PKW und mitgeführte Sachen in Augenschein zu nehmen (rein zu schauen), auch um z.B. „unerlaubten Aufenthalt" und „illegale Zuwanderung" feststellen. Auch hierfür reichen „tatsächliche Anhaltspunkte" und die Einrichtung solcher Gefahrengebiete ist praktisch unbegrenzt möglich.

Dies bedeutet auch eine Ausweitung rassistischer Polizeikontrollen, wie Silvester in Köln oder täglich an Bahnhöfen. People of Color werden kontrolliert, ihnen wird pauschal unterstellt, kriminell zu sein – Rassismus wird dadurch innerhalb und außerhalb der Polizei verstärkt.

Auch Punks und Obdachlose, kurzum alle, die sich anders verhalten oder anders aussehen als die von der Polizei definierte Normalität werden so häufigen diskriminierenden und demütigenden Polizeikontrollen ausgesetzt. Das erzeugt einen hohen Anpassungsdruck und schränkt so natürlich auch faktisch Möglichkeiten sich frei zu entfalten ein.

3. Ausweitung der Möglichkeiten, **Videobeobachtung** an einzelnen öffentlichen Plätzen und bestimmten Orten durchzuführen (Änderungen in § 15a PolG NRW – E)

Damit soll die Videoüberwachung an öffentlich zugänglichen Orten eingeführt werden, wenn die Annahme gerechtfertigt ist, dass Straftaten begangen werden oder „an diesem Ort" Straftaten von erheblicher Bedeutung „verabredet, vorbereitet werden". Das schließt auch Objektüberwachung mit ein, auch das ist ein „Ort".

Bisher waren konkrete Erfahrungen mit Straftaten notwendig, um Orte zu überwachen. Die Ausweitung der Videoüberwachung führt zu einem Überwachungsstaat, in dem es keine unbeobachteten Orte und Momente mehr gibt. Das führt zu einer Verhaltensänderung und Anpassung der sich stets beobachtet Fühlenden.

4. Einführung einer Vorschrift zur **präventiv-polizeilichen Telekommunikationsüberwachung**, einschließlich der Befugnis, auf verschlüsselte Telekommunikationsinhalte mittels Eingriff in informationstechnische Systeme zuzugreifen (NRW- Staatstrojaner, so genannte Quellen-TKÜ).
(Änderungen in § 20c PolG NRW – E)

Die präventiv-polizeilichen Telekommunikationsüberwachung soll bei drohender Gefahr, bei drohender terroristischer Gefahr, aber auch schon beim Verdacht Mitteilungen entgegen zu nehmen oder zu übermitteln eingeleitet werden können und praktisch unbegrenzt fortgeführt werden können.

Die Entgrenzung der kompletten Überwachung auf präventive Zwecke ermöglicht der Polizei zu entscheiden, wer überwacht wird und schafft ihr praktisch geheimdienstliche Befugnisse. Bisher war es Aufgabe der Geheimdienste, extremistische Tendenzen zu erkennen und Aufgabe der Polizei nach Straftaten zu ermitteln. Dieses Trennungsgebot wurde nach den Erfahrungen mit der Gestapo aus gutem Grund eingeführt – eine Vermischung von geheimdienstlichen und polizeilichen Befugnissen führt dazu, dass die Polizei immer mehr politisch entscheidet, wer gerade überwacht wird und zu einem eigenen politischen Akteur wird.

5. Einführung einer strafbewehrten präventiv-polizeilichen Rechtsgrundlage, um gegen mutmaßliche Gefährder **orts- und gebietsbezogene Aufenthaltsanordnungen oder Kontaktverbote** zu erlassen (Änderungen in § 34b PolG NRW – E)

Bei drohender Gefahr ist es er Polizei möglich, Aufenthaltsgebote (z.B. das Verbot den Wohnort zu verlassen) oder Aufenthaltsverbote (also bestimmte Orte nicht zu betreten) zu verhängen und den Kontakt mit bestimmten Personen oder Personengruppen zu verbieten. Auf Antrag der Polizei wird dies vom Amtsgericht angeordnet (oder bei Gefahr im Verzug im Nachhinein bestätigt) und darf jeweils um 3 Monate unbegrenzt verlängert werden. Bei Verstoß gegen Kontakt oder Aufenthaltsverbot droht eine Freiheitsstrafe bis zu zwei Jahren.

Dieses Gesetz bedeutet eine massive Beschränkung der Freizügigkeit. Der Staat kann Personen praktisch an ihrem Wohnort einsperren oder ihnen verbieten, sich mit anderen Menschen zu treffen oder auch nur zu telefonieren. Damit findet auch eine Einschränkung der freien Meinungsäußerung statt, es wird verboten mit bestimmten Menschen sich auszutauschen und zu diskutieren. Wohlgemerkt all das, ohne dass die Personen eine Straftat begangen haben, rein zu präventiven Zwecken. Diese Machtbefugnisse sind in der BRD einzigartig. Damit wird die Bestrafung ins Vorfeld verlagert, schon von der Staatslinie stark abweichende Haltungen, die z.B. das staatliche Gewaltmonopol in Frage stellen, können so bestraft werden.

6. Einführung einer strafbewehrten präventiv-polizeilichen Rechtsgrundlage zur Anordnung einer **elektronischen Aufenthaltsüberwachung** („Elektronische Fußfessel") (Änderungen in § 34c PolG NRW – E)

Die elektronische Aufenthaltsüberwachung mit Fußfessel ist gedacht zur Verhütung oder Verfolgung von Straftaten von erheblicher Bedeutung, Feststellen von Verstößen gegen Aufenthaltsvorgaben und Kontaktverboten, zur Verfolgung von Straftaten, Abwehr von erheblichen Gefahren für Leib, Leben und Freiheit von Personen. Auch sie darf praktisch unbegrenzt angeordnet werden. Ein Verstoß gegen die Anweisung sie zu tragen, führt zu einer Gefängnisstrafe von bis zu zwei Jahren.

Bisher wurde die elektronische Fußfessel als Freiheitsstrafe gewertet, als Alternative zum Gefängnis oder zur Überwachung von Bewährungsauflagen

– also nach rechtskräftigen Verurteilungen eingesetzt. Jetzt soll auch sie bereits präventiv bei drohenden Gefahren eingesetzt werden. Das heißt: Menschen werden total überwacht ohne je eine Straftat begangen zu haben, lediglich weil die Polizei glaubt, sie könnten dies tun. Das stellt eine erhebliche Grundrechtseinschränkung dar, da zum einen ein freies Bewegen und freie Entscheidungen unmöglich werden, zum anderen weil die Sichtbarkeit der Überwachung durch die elektronische Fußfessel sofort zu Diskriminierungen führt. Das repressive Potenzial auch für Überwachung und Einschränkung einer politischen Opposition ist nahezu unbegrenzt.

7. Ergänzung der Vorschriften um die **Ingewahrsamnahme**, um weitere Möglichkeiten der Ingewahrsamnahme sowie Ermöglichung einer Verlängerung des Gewahrsams zur Gefahrenabwehr auf Grund des Polizeigesetzes (Änderungen in § 38 PolG NRW – E)

Auch bei drohender Gefahr und drohender terroristischer Gefahr wird eine Ingewahrsamnahme zur Gefahrenabwehr ermöglicht. Die mögliche Länge von Gewahrsam wird bei drohender terroristischer Gefahr oder Verstoß gegen Aufenthaltsbeschränkungen oder Kontaktverbot auf einen Monat verlängert und in weiteren Fällen auf 7 Tage ausgeweitet, auch zur bloßen Identitätsfeststellung (wenn diese erschwert wird, d.h. keine Personendaten von Betroffenen angegeben werden).

Die Ingewahrsamnahme ist ein Freiheitsentzug. Dieser wird nun deutlich ausgeweitet auch in den Fällen, in denen bloße Verdachtsmomente vorliegen. Besonders begründet wird im Gesetzesentwurf die Ingewahrsamnahme bis zu 7 Tagen zur reinen Identitätsfeststellung. Da es hier um Fälle geht, in denen keine ausreichenden Verdachtsmomente für Straftaten vorliegen, die eine Untersuchungshaft rechtfertigen, ist das klar unverhältnismäßig.

8. Ergänzung des *Waffenkatalogs um Distanzelektroimpulsgeräte* (**„Taser“**) (Änderungen in § 58 PolG NRW – E)

Taser sind gefährliche Waffen und führen immer wieder zu Todesfällen. Dadurch, dass sie von der Polizei als nichttödlich eingeschätzt werden und die Einsatzhemmschwelle nicht so groß ist, steigt die Gefahr von schweren Verletzungen und Tötungen. Notwendig sind die Taser nicht, der Polizei stehen bereits jetzt genug Waffen zur Verfügung. Statt einer Aufrüstung ist mehr Training in Deeskalation und Kommunikation notwendig.

Mit dem Gesetz soll die Sicherheit der Bürgerinnen und Bürger gestärkt werden, dabei führen gerade die Ausweitung der Befugnisse der Polizei zu einer verstärkten Unsicherheit derjenigen, die von der Polizei nicht als schützenswert angesehen werden. Das Gesetz trägt also weiter zur Diskriminierung bei. Gegen Terrorismus dürfte es zudem wenig helfen, da hier die Täter*innen oft gerade nach Aufmerksamkeit streben und eine Überwachung oder Fußfessel sie bewiesenermaßen nicht abhält. Hier wird eine nicht-existente Sicherheit vorgespiegelt um weitere Grundrechtseinschränkungen, die Erweiterung der Polizei um geheimdienstliche Befugnisse und die Transformation in einen Polizeistaat zu rechtfertigen.

Deshalb lehnen wir das Gesetz ab.

Quelle:
https://freiheitsfoo.de/2018/03/14/rise-of-the-police-nrw/

Bündnis Brementrojaner gegen Verschärfung des Bremischen Polizeigesetzes 04.04.2018

Das Bremische Polizeigesetz soll verschärft werden: Das Bündnis Brementrojaner stellt sich dem entgegen. Kein weiterer Abbau von Grundrechten!

In Bremen treibt die rot-grüne Landesregierung im Eiltempo und ohne gesellschaftliche Debatte eine folgenschwere Änderung des Bremischen Polizeigesetzes voran. Der Senator für Inneres hat einen entsprechenden Gesetzentwurf am 15.12.2017 vorgelegt. Er sieht gravierende rechtsstaatliche, grund- und datenschutzrechtliche Eingriffe vor.

Seit der ersten öffentlichen Debatte in der Innendeputation am 10. Januar 2018 steht der Entwurf des Innensenators in der öffentlichen Kritik. Inzwischen haben die rot-grünen Koalitionspartner den Entwurf intern überarbeitet; über das Ergebnis wird wahrscheinlich am 12.04.2018 in der Innendeputation abgestimmt. Auch nach möglichen Änderungen durch die rot-grüne Koalition wird unsere grundsätzliche Kritik an der Verschärfung des Bremischen Polizeigesetzes bestehen bleiben.

Denn die Konsequenzen sind:

- weitreichender Ausbau staatlicher Videoüberwachung im öffentlichen Raum
- Einführung von „elektronischen Fußfesseln“ zur lückenlosen Aufenthaltskontrolle mutmaßlicher „Gefährder“ – also von Menschen, die nicht etwa Straftaten begangen haben, sondern denen solche aufgrund bestimmter Anhaltspunkte lediglich zugetraut werden
- massive Ausweitung der polizeilichen Überwachung elektronischer Kommunikation mittels Computern und Smartphones, insbesondere durch heimlich eingeschleuste Schadsoftware („Staatstrojaner“)

Das *Bündnis Brementrojaner* ist ein Zusammenschluss verschiedener zivilgesellschaftlicher und politischer Gruppen und Personen. Wir lehnen die geplante massive Überwachung und die damit einhergehenden gravierenden Grundrechtseingriffe entschieden ab. Die vorgeblich notwendigen Sicherheitsverschärfungen sind unverhältnis-

mäßig und widersprechen rechtsstaatlichen Prinzipien. **Susanne Wendland, Mitglied der Bremischen Bürgerschaft (parteilos)** und Sprecherin für das Bündnis: *„Es geht um unsere freiheitlich demokratische Grundordnung. Um unsere Freiheits- und Grundrechte, die angegriffen werden. Schlimmer noch: Sie werden ignoriert. Um uns vorzugaukeln, wir hätten die terroristische Gefahr im Griff. Sicherheitsfolklore nenne ich das, die zu nichts taugt. Deswegen lehnen wir als Bündnis die geplante Gesetzesverschärfung vollständig ab*.“

Die geplante Erweiterung von Videoüberwachung ist nicht hinzunehmen. *„Bereits jetzt ist Videoüberwachung in Bremen weit verbreitet, obwohl ein entsprechender Nutzen nicht nachgewiesen ist“*, sagt Bündnissprecherin **Maike Schmidt-Grabia von Digitalcourage e.V. Bremen** *„Noch mehr Kameras werden unsere Freiheit weiter einschränken. Denn wer beobachtet wird, ist nicht frei*.“

Mit dem Argument der Terrorismusabwehr sollen der Polizei weitreichende Grundrechtseingriffe auch in unser aller Privat- und Intimsphäre ermöglicht werden. **Rolf Gössner, Internationale Liga für Menschenrechte** und Bündnissprecher: *„Der Bremer Gesetzentwurf reiht sich mit besonders eingriffsintensiven Polizeibefugnissen in eine bundesweite Entwicklung ein, mit der mühsam errungene Grund- und Freiheitsrechte abermals massiv eingeschränkt werden, um vermeintlich mehr Sicherheit zu erreichen. Insgesamt ein weiterer, verfassungsrechtlich hoch problematischer Schritt in Richtung präventiver Sicherheitsstaat*.“

Eingeschränkt werden die Freiheitsrechte u.a. durch das heimliche Einschleusen von „Staatstrojanern“ in Computer und Smartphones. Der Staatstrojaner zerstört das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen. Dazu sagt Bündnissprecher **Aaron Lye vom Forum Informatiker_Innen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)**: *„Eingriffe in Rechnersysteme als Ermittlungsinstrument stellen strukturelle Gefahren für IT-Systeme und damit letztendlich für uns alle dar. Denn sie öffnen Missbrauch und gefährlichen Attacken Tür und Tor*.“

Das *Bündnis Brementrojaner* verurteilt zudem die Art und Weise, wie der Gesetzentwurf möglichst lautlos durch das Gesetzgebungsverfahren gedrückt werden soll. Eine öffentliche parlamentarische Anhörung von Sachverständigen – wie etwa in Hessen – fand bisher nicht statt. **Susanne Wendland (MdBB)**: *„Es ist vollkommen unverständlich, dass eine rot-grüne Regierungskoalition solche tiefgreifenden Eingriffe in Grund- und Freiheitsrechte plant, ohne zuvor eine breite öffentliche Debatte in der Gesellschaft geführt zu haben*.“

Das Bündnis Brementrojaner fordert die regierenden Parteien dazu auf, den laufenden Gesetzgebungsprozess für das Bremische Polizeigesetz abzubrechen.

Wer Freiheit für Sicherheit aufgibt, wird beides verlieren!

Bündnispartner_Innen: (in alphabetischer Reihenfolge):

- Chaos Computer Club Bremen e.V. (CCCHB)
- Digitalcourage e.V. – Ortsgruppe Bremen
- Forum Informatiker_Innen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
- GRÜNE JUGEND Bremen
- Humanistische Union – Landesverband Bremen (HU)
- Internationale Liga für Menschenrechte e.V. (ILMR)
- Piratenpartei – Landesverband Bremen
- ver.di – Ortsverein Bremen
- Verein für Rechtshilfe im Justizvollzug des Landes Bremen e.V.
- Susanne Wendland, Mitglied der Bremischen Bürgerschaft (parteilos)
- Elke Bahl u. Prof. Dr. Helmut Pollähne vom Kriminalpolitischen Arbeitskreis Bremen (kripak)

Quelle:
https://brementrojaner.de/index.php/startseite/

Geplante Verschärfungen des hessischen Verfassungsschutzgesetzes schädigen Demokratie und Grundrechte

Gemeinsame Erklärung warnt vor schwarz-grüner Gesetzesnovelle: Geplante Verschärfungen des hessischen Verfassungsschutzgesetzes schädigen Demokratie und Grundrechte vom 24.12.2017

Das geplante Verfassungsschutzgesetz für Hessen ist die freiheitsfeindlichste Regelung zur Arbeit eines Geheimdiensts in Deutschland. Sorgen bereitet Bürgerrechtsorganisationen, Datenschützern und Demokratieprojekten sowie vielen Menschen die damit drohende Gefahr für Meinungsfreiheit, Informationelle Selbstbestimmung, Datenschutz, Rechtsstaat und Demokratie.

Befremden hat auch die Haltung der Grünen-Fraktion im Hessischen Landtag ausgelöst. Trotz eines ablehnenden Beschlusses der Grünen Landesmitgliederversammlung am 18.11.2017 in Hanau treiben die grünen Regierungsmitglieder und Parlamentarier das Gesetzgebungsverfahren im Eiltempo durch den Hessischen Landtag. Dabei drohen zahlreiche schwerwiegende Folgen, die bisher noch gar nicht alle öffentlich diskutiert wurden. Schon die vier wichtigsten Kritikpunkte machen deutlich, warum nicht nur die Grüne Basis dieses Gesetz ablehnt:

1. Der Gesetzentwurf vom 14.11.2017 sieht den heimlichen Einsatz sogenannter Trojaner vor. Sie nutzen Lücken in Programmen und Apps, um unbemerkt vom angegriffenen Nutzer Smartphones, Computer oder andere – mit dem Internet verbundene – Geräte zu kontrollieren. Durch die Nutzung von Trojanern gerät der Staat in ein moralisches Dilemma: Zwar möchte er auf der einen Seite angesichts der zunehmenden Bedrohungslage die IT-Sicherheit von Privatpersonen und

Unternehmen fördern, andererseits hat er aber auch ein starkes Interesse an einem Fortbestand solcher Sicherheitslücken. Finanziert mit Steuergeldern werden sie möglichst lange vor den Herstellern der Programme und Apps geheim gehalten. Weil deshalb nicht nur der Verfassungsschutz, sondern auch Internet-Kriminelle diese Lücken ausnutzen können, ermöglicht und fördert der Staat damit letztlich auch ihre Verbrechen. Der „Hessentrojaner" gefährdet deshalb weltweit informationstechnische Systeme sowie die Integrität und Vertraulichkeit digitaler Kommunikation, wie sie per Grundgesetz und nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) eigentlich besonders geschützt werden sollen. Terroristische Anschläge in den Ländern mit den schärfsten Abhör- und Überwachungsgesetzen zeigen, dass solche Trojaner keinen Bürger vor Gewalt schützen. Mit ihrer Hilfe werden eher ungefährliche Oppositionelle verfolgt oder eingeschüchtert.

2. Künftig soll das Hessische Landesamt für Verfassungsschutz (LfV) Personen überprüfen, die in Projekten zur Abwehr von Islamismus, Rechtsradikalismus und anderen demokratierelevanten Bereichen durch Landesmittel gefördert werden. Der hessische Verfassungsschutz erhält hier also den Auftrag, auch die Gegner der Extremisten zu erfassen. Dabei benutzt er nach wie vor einen fragwürdigen Extremismusbegriff. Die Beschäftigten bei solchen Projekten lehnen diese Gesinnungsschnüffelei zu Recht ab, die an unselige Zeiten der Berufsverbote erinnert. Im Falle einer Verweigerung droht ihnen der Entzug der Fördergelder oder sonst der Verlust ihres qualifizierten Personals.

3. Auch weiterhin soll der Verfassungsschutz in Hessen systematisch V-Leute einsetzen können. Selbst vorbestrafte Kriminelle können als Zuträger aktiviert werden, wenn die Führungsebene des Landesamts ihren Einsatz befürwortet. Damit unterstützt eine staatliche Behörde Kriminelle und fördert deren rechtswidriges Handeln.

4. Obwohl der Mord an Halit Yozgat in Kassel und die Rolle des Landesamts für Verfassungsschutz mitsamt seines damaligen V-Mann-Führers Andreas Temme sowie die Rolle des damaligen Innenministers Volker Bouffier immer noch nicht lückenlos aufgeklärt sind und zahlreiche Widersprüche und nachweisbare Falschaussagen bislang keinerlei Konsequenzen gezeigt haben, will die Landesregierung den Verfassungsschutz in Hessen durch zusätzliche Befugnisse und technische Ausstattung weiter stärken. Die im Gesetzentwurf vorgesehene parlamentarische Kontrolle des Inlandsgeheimdienstes ist indes sehr lückenhaft und muss angesichts von dessen Aufrüstung und Stärkung weitgehend ins Leere laufen.

Die Regierungsmehrheit bestimmt, wer in der Parlamentarischen Kontrollkommission (PKK) vertreten ist und hat dort die Mehrheit. Zudem bestehen kaum Dokumentationspflichten, die eine wirksamere Überprüfung der Aktivitäten des Geheimdienstes durch die Parlamentarische Kontrollkommission oder durch Gerichte gewährleisten könnten.

Angst vor Terror darf nicht zum Abbau von Demokratie und Bürgerrechten führen. Ein kaum zu erwartender Erkenntnisgewinn darf nicht durch die massive Einschränkung von Freiheitsrechten wie beim vorliegenden Entwurf zum Hessischen Verfassungsschutzgesetz erkauft werden. Insbesondere der Respekt vor den Opfern des „Nationalsozialistischen Untergrunds" (NSU) und die Lehren aus den Verfassungsschutzskandalen gebieten die konsequente Verfolgung aller Verantwortlichen einschließlich von Mitarbeitern des Verfassungsschutzes sowie dessen angemessene Reform und „rechtsstaatliche Zähmung".

Auch der Mitte Dezember 2017 aufgrund öffentlichen Drucks nachgeschobene „eilige Entschließungsantrag" der Regierungskoalition bleibt nur ein Lippenbekenntnis. Darin betonen CDU und Grüne zwar, dass die Präventionsarbeit nur gelingen könne, wenn sie von Vertrauen getragen wird; gleichzeitig beharren sie aber weiterhin auf der Einbeziehung nachrichtendienstlicher Erkenntnisse als angebliche Voraussetzung für solches Vertrauen. Das Vertrauen in seine demokratische Ausrichtung hat der Geheimdienst aber spätestens durch seine Vertuschungsaktionen während der Aufarbeitung der NSU-Morde endgültig verspielt.

Angesichts dieser und vieler weiterer Bedenken fordern wir Die Grünen und den gesamten Hessischen Landtag auf, das Gesetzgebungsverfahren abzubrechen und dem vorliegenden Gesetzentwurf nicht zuzustimmen. Keinesfalls dürfen Die Grünen in Hessen den Weg in den Überwachungsstaat ebnen.

Initiiert durch die Humanistische Union und die Internationale Liga für Menschenrechte

Unterstützer:

1. Arbeitskreis Barrierefreies Internet (AKBI) e.V. (http://www.akbi.de)
2. Chaos Computerclub Darmstadt (http://darmstadt.ccc.de)
3. Die Datenschützer Rhein-Main (http://www.ddrm.de)
4. Die Linke Hessen (http://www.die-linke-hessen.de)
5. Digitalcourage e.V. (http://www.digitalcourage.de)
6. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) (www.fiff.de/)
7. Freifunk Marburg (https://marburg.freifunk.net)
8. Humanistische Union Frankfurt (http://frankfurt.humanistische-union.de)
9. Humanistische Union, Landesverband Hessen (http://www.hu-hessen.de)
10. Humanistische Union Marburg (http://www.hu-marburg.de)
11. Internationale Liga für Menschenrechte (https://www.ilmr.de)
12. Komitee für Grundrechte und Demokratie (http://www.grundrechtekomitee.de)
13. Linke Fraktion im Hessischen Landtag (http://www.linksfraktion-hessen.de)
14. Marburger Initiative gegen den Überwachungsstaat (http://www.miguest.de)
15. Piratenpartei Hessen (https://www.piratenpartei-hessen.de)

Quellen:

https://ilmr.de/2017/geplante-verscharfungen-des-hessischen-verfassungsschutzgesetzes-schadigen-demokratie-und-grundrechte-gemeinsame-erklarung-von-burgerrechts-und-datenschutzverbanden

https://freiheitsfoo.de/2018/02/01/erklaerung-gegen-staerkung-hessischen-inlandsgeheimdienstes/

Berliner Allianz für Freiheitsrechte zur Sicherung grundgesetzlich garantierter Freiheit hat sich gegründet!

Am 11. April 2018 hat sich die Berliner Allianz für Freiheitsrechte gegen das von Thomas Heilmann, Heinz Buschkowsky und anderen angestrebte Volksbegehren gegründet. Die Berliner Allianz für Freiheitsrechte will, dass sich Parteien und Zivilgesellschaft gleichermaßen gegen den Ausbau von Videoüberwachung und für die Freiheitsrechte der Menschen einsetzen.

Max Althoff, Rechtsanwalt, erklärt dazu: „Die geplante massenhafte Videoüberwachung der Initiative mit dem irreführenden Namen ‚Aktionsbündnis für mehr Videoaufklärung und Datenschutz‘ stellt die Menschen unter Generalverdacht, schafft Misstrauen und verändert die Art, wie wir miteinander umgehen. Eine Ausweitung der Videoüberwachung oder gar eine Tonüberwachung im öffentlichen Raum lehnen wir daher ab. Videoüberwachung ist der Einstieg in ein umfassendes Überwachungssystem für mehr Kontrolle über jeden von uns."

Maximilian Blum, Sprecher der LAG Netzpolitik der Linken, ergänzt: „Mit der vom Volksbegehren angestrebten ‚intelligenten Technik‘ der Videoüberwachung sollen mittels eines ‚speziellen Algorithmus‘ ‚potentiell gefährliche Situationen‘ in ‚automatischer Früherkennung‘ identifiziert werden. Hieraus geht eindeutig hervor, dass es nicht nur um Täteraufklärung geht, sondern um die massenhafte Überwachung von Personen, denen ausgehend von entsprechenden Algorithmen ein mehr oder weniger großes Potential zur Begehung einer Straftat pauschal zugesprochen wird. Eine so umfassende Überwachungstechnologie schlägt schnell von einer Verhaltensanalyse in eine Verhaltenssteuerung um."

Aus Sicht der Berliner Allianz für Freiheitsrechte führt ein Ausbau der Videoüberwachung niemals zu mehr Sicherheit. „Sie kann nur ein rein subjektives Unsicherheitsgefühl beruhigen, führt letztendlich aber nur zur Verlagerung der Kriminalität an andere Orte", so Thilo Weichert vom Netzwerk Datenschutzexpertise. „Zielgerechter wäre es, wenn die Ursachen der Probleme analysiert würden und die Politik sich aktiv mit deren Beseitigung beschäftigte, anstatt weiter auf eine Politik der Verdrängung und Repression zu setzen."

Alexander Spies, der ehemalige Vorsitzende der Piratenfraktion im Abgeordnetenhaus, ergänzt: „Mit der Fokussierung auf Videoüberwachung machen sich die Initiatoren einen schlanken Fuß, führen die Menschen und ihre Sorgen in die Irre und verweigern tatsächliche Antworten auf sicherheitspolitische Fragestellungen. Damit setzt das Volksbegehren den Weg der Berliner CDU fort, den diese schon als Teil des Senats verfolgte: die reine Verschleppung der Probleme."

Auch das massenhafte Speichern von Daten stößt bei der Berliner Allianz für Freiheitsrechte auf erhebliche Kritik. Dazu Werner Hülsmann, stellvertretender Vorsitzender der Deutschen Vereinigung für Datenschutz: „Es ist bekannt, dass das massenhafte Speichern von Daten weitere Begehrlichkeiten weckt und immer auch die Gefahr birgt, dass diese abhanden kommen. Das Grundrecht auf Datenschutz und informationelle Selbstbestimmung kann bei Nutzung so einer Masseninfrastruktur nicht garantiert werden. Deshalb stellt ein Ausbau der Überwachung sogar ein erhöhtes Sicherheitsrisiko dar. Die gewonnenen Ton- und Videodaten werden aufgrund der riesigen Masse nur automatisch ausgewertet. Ob hier Ballspiele von Schlägereien unterschieden werden können, ist höchst fraglich. Ein direktes Eingreifen bei einer Gefahr findet nicht statt, weil Kameras niemals eingreifen und einer bedrängten Person helfen können. Das bringt kein Mehr an Sicherheit, und auch keine Polizist*in ist bei einer gefährlichen Situation tatsächlich vor Ort."

Auch rechtlich sei das Volksbegehren zweifelhaft. Louisa Hattendorff, Sprecherin der Grünen Jugend Berlin, führt aus: „Das Volksbegehren weckt erhebliche verfassungsrechtliche Bedenken. Es sollen auch massenhaft Tonaufnahmen erhoben und einen Monat gespeichert werden. Der Gesetzeswortlaut lässt jede Verhältnismäßigkeit vermissen. Es ist ein Treppenwitz der Geschichte, dass gerade ein ehemaliger Justizsenator so leichtfertig mit den Grenzen unseres Grundgesetzes und den Freiheiten der Menschen umgeht."

Rebecca Cotton sagt: „Wir wollen, dass der Schutz der Privatsphäre, welche sich in Verbindung mit dem einzigen nicht einschränkbaren Grundrecht, der Menschenwürde, aus der Verfassung ableitet (Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG), erhalten bleibt. Dieser Schutz darf nicht unter dem Deckmantel der Sicherheit der Bürger*innen zur Ausweitung der Macht und Informationshoheit des Staates ausgehöhlt werden."

Axel Bussmer von der Humanistischen Union ergänzt: „Aufgrund der zahlreichen, inzwischen von Fachleuten, der Berliner Beauftragten für Datenschutz und Informationsfreiheit und Verbänden geäußerten verfassungsrechtlichen Bedenken fordern wir die Senatsverwaltung auf, das Gesetzesvorhaben dem Verfassungsgerichtshof des Landes Berlin zur rechtlichen Prüfung vorzulegen und keine Gespräche mit dem Überwachungsbündnis zu führen."

Der Gründungsaufruf der Berliner Allianz für Freiheitsrechte:

Berliner Allianz für Freiheitsrechte fordert: Nein zur Ton- und Videoüberwachung an öffentlichen Orten

Jedes Jahr wächst Berlin um mehrere zehntausend Menschen. Jedes Jahr besuchen mehr Tourist*innen als im Vorjahr die Hauptstadt, während die Verbrechenszahlen insgesamt nicht steigen. Letztes Jahr sanken sie sogar.

Wir wollen, dass Berlin weiterhin eine weltoffene, lebenswerte, freie und sichere Stadt für alle bleibt. Egal ob Sie in Berlin geboren, zugezogen oder nur zu Besuch sind. Egal ob Sie alt oder



Bild: AdobeStock

jung, arm oder reich, gläubig oder ungläubig sind.

Damit dies so bleibt, sind wir für alle zielgerichteten Vorschläge offen.

Aber der Vorschlag der Überwachungsinitiative mit dem irreführenden Namen „Aktionsbündnis für mehr Videoaufklärung und Datenschutz" trägt nicht dazu bei, die Freiheit und Sicherheit in Berlin zu verbessern. Der Gesetzesvorschlag des Überwachungsbündnisses, über den wahlberechtigte Berliner*innen eventuell 2019 abstimmen könnten, verstößt an mehreren Punkten gegen das Recht auf informationelle Selbstbestimmung, gegen elementare Grundrechte und unser Verständnis einer freien Gesellschaft.

Was das Überwachungsbündnis will – und warum das kein Beitrag zur Sicherheit ist

Das Überwachungsbündnis will das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG Bln) so ändern, dass in Berlin prinzipiell an allen öffentlichen Orten eine Ton- und Videoüberwachung möglich ist. Das Überwachungsbündnis will alle Orte, an denen Straftaten geschehen, geschehen könnten, verabredet oder vorbereitet werden oder an denen große Menschenmengen sind, überwachen.

Das soll in Berlin mit bis zu 2500 Kameras an 50 öffentlichen Plätzen geschehen. Die Orte sollen von der Polizei in Zusammenarbeit mit dem zu gründenden Berliner Institut für Kriminalprävention festgelegt werden. Das Institut soll, in der von der Überwachungsinitiative vorgeschlagenen Form, nur Vorschläge zum Einsatz der Videoüberwachung machen. Es wird nicht wissenschaftlich arbeiten und verstößt gegen verfassungs- und europarechtliche Vorgaben zur Datenschutzaufsicht.

Außerdem sollen 300 große Fahrradabstellplätze überwacht werden. Diese Zahlen werden in den Fußnoten des Gesetzesentwurfs genannt, mit dem in den vergangenen Monaten Unterschriften gesammelt wurden. Mögliche Orte nennt das Überwachungsbündnis nicht. Die Zahl der Kameras, etwa fünfzig pro Ort, wird ebenfalls nicht begründet.

Die Bild- und Tonüberwachung kann, so die Überwachungsinitiative, auch geheim erfolgen. Es soll, ohne eine öffentliche Diskussion, immer die modernste Technik und möglichst „intelligente" Videoüberwachung eingesetzt werden. So sollen Verbrechen ausschließlich mit technischer Hilfe aufgeklärt und verhindert werden.

Mit der vom Volksbegehren angestrebten „intelligenten" Videoüberwachung wird die Unschuldsvermutung missachtet und jeder Mensch im öffentlichen Raum als potentielle Straftäter*in betrachtet. Mittels Algorithmen sollen „akut gefährliche Situationen" automatisch erkannt werden. Es geht um die Überwachung von Personen, die aufgrund der Prognosen von Algorithmen Straftaten begehen könnten. Oder sich einfach nur auffällig verhalten. Dafür sollen alle Personen, die sich an einem Ort aufhalten, überwacht und ihre Gespräche abgehört werden. Dies ist vollkommen unangemessen und nach geltendem Recht auch nicht verhältnismäßig. Zudem geht mit einer solchen umfassenden Überwachungstechnologie eine große Missbrauchsgefahr einher.

Bisherige Erfahrungen mit der Videoüberwachung sprechen gegen die vollmundigen Versprechen der Über-

wachungsinitiative, dass durch Videokameras Verbrechen verhindert werden können.

Wenn die Kameras allerdings vor allem zur Aufklärung von Verbrechen eingesetzt werden sollen, fehlt dem Land Berlin die Gesetzgebungskompetenz.

Warum die Berliner Allianz für Freiheitsrechte den Gesetzesvorschlag ablehnt

Das Überwachungsbündnis möchte die Bild- und Tonaufnahmen einen Monat lang speichern. Verschiedene datenschutzrechtliche Regelungen sehen jedoch vor, dass Videoaufnahmen unverzüglich zu löschen sind. Derzeit speichert die BVG Bildaufnahmen 48 Stunden lang. Tonaufnahmen fertigt sie überhaupt nicht an.

Das Speichern von Tonaufnahmen ist ein akustischer Lauschangriff, der nur in sehr wenigen Fällen mit hohen juristischen Hürden erlaubt ist. Nach geltendem Strafprozessrecht muss die belauschte Person - auch wenn sie in der Öffentlichkeit abgehört werden soll - verdächtig sein, eine bestimmte Tat begangen zu haben.

Das Land Berlin hat im Bereich der Strafprozessordnung keine gesetzgeberische Kompetenz. Es kann eine so weitreichende Regel, die alle Menschen betrifft, die sich im Umfeld einer nicht zwingend gekennzeichneten Bild- und Tonüberwachung aufhalten, nicht beschließen.

Die Berliner Allianz für Freiheitsrechte fordert: Keine Verhandlungen über diesen Gesetzesvorschlag

Wir, die Unterzeichnenden, halten den Vorschlag des Überwachungsbündnisses für einen gefährlichen Irrweg. Er verstößt gegen elementare Freiheitsrechte und führt nicht zu mehr Sicherheit.

Deshalb lehnen wir diesen unverhältnismäßigen und sehr wahrscheinlich verfassungswidrigen Gesetzesentwurf ab.

Wir, die Berliner Allianz für Freiheitsrechte, fordern den Senat auf, den Vorschlag der Überwachungsinitiative durch den Verfassungsgerichtshof des Landes Berlin prüfen zu lassen.

Wir fordern die Regierungsparteien auf, nicht mit dem Überwachungsbündnis zu verhandeln.

Wir fordern die im Abgeordnetenhaus vertretenen Parteien auf, den Gesetzesentwurf der Überwachungsinitiative entschieden abzulehnen.

Die Gründungsmitglieder der Berliner Allianz für Freiheitsrechte und Erstunterzeichner*innen dieses Aufrufs sind:

Organisationen: Aktion Freiheit statt Angst e.V., Berlin-Mitte gegen Überwachung, Datenschutzraum e.V., Deutsche Vereinigung für Datenschutz (DVD) e.V., Digitalcourage e. V., Fanrechtefonds, Humanistische Union e. V. (Landesverband Berlin-Brandenburg), Internationalen Liga für Menschenrechte e. V.

Parteigliederungen: Bündnis 90/Die Grünen (Kreisverband Friedrichshain-Kreuzberg), Bündnis 90/Die Grünen (Landesarbeitsgemeinschaft Netzpolitik), DIE LINKE Berlin (Landesarbeitsgemeinschaft Bürgerrechte & Demokratie), DIE LINKE Berlin (Landesarbeitsgemeinschaft Netzpolitik), Grüne Jugend Berlin, Junge Liberale Berlin

Privatpersonen: Rebecca Cotton, Christian Demmelmeier (Jurist), Dr. Rolf Gössner (Rechtsanwalt/Publizist, Internationale Liga für Menschenrechte), Rainer Hammerschmidt, Arno Hoffmann, Viktoria Kleinbongartz (Volljuristin), Herbert Nebel, Felix Rauch (Rechtsanwalt), Niklas Schrader (MdA, Sprecher für Datenschutz, Verfassungsschutz und Drogenpolitik für die Fraktion DIE LINKE im Abgeordnetenhaus von Berlin), Thilo Weichert (Netzwerk Datenschutzexpertise), Evelyn Westhoff

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kartellamt begründet Vorgehen gegen Facebook

Weil Facebook in Deutschland den Markt der sozialen Netzwerke beherrscht, hat das Bundeskartellamt als Aufsichtsbehörde in dem gegen den Konzern laufenden Verfahren wegen des „Verdachts auf Missbrauch einer marktbeherrschenden Stellung“ am 19.12.2017 seine vorläufige rechtliche Einschätzung mitgeteilt. Es vertritt darin die Ansicht, dass das Unternehmen missbräuchlich handelt, indem es die Nutzung des Netzwerks „davon abhängig macht, unbegrenzt jegliche Art von Nutzerdaten aus Drittquellen sammeln und mit dem Facebook-Konto zusammenführen zu dürfen“.

Zu diesen Drittseiten gehören neben konzerneigenen Diensten wie WhatsApp oder Instagram auch Webseiten und Apps anderer Betreiber, auf die Facebook über Schnittstellen zugreifen kann. Solche Schnittstellen können sichtbar werden, wenn etwa Facebooks Like-Button in die Angebote anderer Webseiten eingebunden ist. Besonders deutlich wird die Verknüpfung dann, wenn Nutzende etwa auf Nachrichtenseiten aus der Website heraus mit ihrem Facebook-Account Kommentare verfassen können. Oft wird dann unter Artikeln oder Postings schon das eigene Profilbild sichtbar. Grund ist, dass man mit demselben Browser auf Facebook eingeloggt ist. Die Nutzeraktivität wird dann an Facebook übermittelt, dort gesammelt und verwertet. Die Wettbewerbshüter kritisieren, dass es nicht einmal nötig ist, dass Schnittstellen zu Facebook aktiv angeklickt werden; es genügt schon der Besuch einer externen Seite, dass Facebook dies speichern kann.

Facebook ist mit Abstand das größte soziale Netzwerk, das über seine Schnittstellen weit ins Internet ausgreift. Diese Allgegenwart macht es Nutzenden nach Ansicht des Kartellamts praktisch unmöglich, zu einem anderen Anbieter zu wechseln. Für andere Unternehmen sei es kaum möglich, Konkurrenzangebote zu etablieren. Weil Facebook kostenlos sei, gebe es zwar keine finanziellen Nachteile für die Nutzenden. Der Schaden liege „in einem Kontrollverlust für den Nutzer: Er kann nicht mehr selbstbestimmt über seine persönlichen Daten verfügen.“ Dies sei keine reine Frage des Datenschutzes, sondern auch eine kartellrechtliche: Bei Netzwerk-Unternehmen kann der „Zugang zu wettbewerbsrelevanten Daten“ laut Gesetz Grund für eine marktbeherrschende Stellung sein. Das Kartellamt spricht von einem „Quasi-Monopol von Facebook mit mehr als 90 Prozent der Nutzeranteile“.

Kartellamtspräsident Andreas Mundt erläuterte: „Wir sehen vor allem die Datensammlung außerhalb des sozialen Netzwerks von Facebook und ihre Zusammenführung mit dem Facebook-Konto als problematisch an“. Dass dann Nutzerdaten an Facebook fließen, sei den Nutzenden nicht bewusst. Facebook müsse als marktbeherrschendes Unternehmen bei seinem Geschäftsmodell berücksichtigen, dass die Nutzenden nicht auf andere soziale Netzwerke ausweichen könnten. Mundt bemängelte, dass für das Vorgehen von Facebook keine rechtliche Grundlage besteht: „Wir sehen nach dem jetzigen Stand der Dinge auch nicht, dass zu diesem Verhalten von Facebook, dem Daten-Tracking und der Zusammenführung mit dem Facebook-Konto, eine wirksame Einwilligung der Nutzer vorliegt.“

Die Nutzung von Facebook setzt eine Registrierung und eine uneingeschränkte Zustimmung zu den Nutzungsbedingungen zwingend voraus. Mundt: „Der Nutzer wird vor die Wahl gestellt, entweder das ‚Gesamtpaket‘ zu akzeptieren oder auf die Nutzung des Dienstes zu verzichten“. Nach einer vorläufigen Bewertung seien die Nutzungsbedingungen von Facebook „zumindest in diesem Punkt nicht angemessen“. Sie verstießen zu Lasten der Nutzer gegen den Datenschutz.

Das Kartellamt untersucht seit 2016, ob Facebook als „datengetriebenes Unternehmen“ seine beherrschende Stellung am deutschen Markt ausnutzt (DANA 2/2016, 90). Mundt wies darauf hin, dass das konkrete Kartellverfahren komplex ist: „Wir leisten hier Pionierarbeit“. Das Netzwerk muss nun formell auf die Vorwürfe reagieren, so Munch: „Wir sind mit Facebook im Gespräch. Wenn der Konzern seine Praxis verpflichtend anpasst, würden wir das Verfahren beenden. Anderenfalls können wir auch eine Verfügung gegen Facebook erlassen.“ Vor Frühsommer 2018 ist keine Entscheidung zu erwarten.

Yvonne Cunanne, europäische Datenschutzchefin des Unternehmens, bestritt, dass Facebook in Deutschland marktbeherrschend sein: „Beliebtheit ist nicht gleich Dominanz.“ Deutsche Nutzende hätten die Wahl andere Netzwerke wie Snapchat zu verwenden. Man halte sich an europäische Datenschutzgrundsätze. Cunnane zufolge gibt es keinen Grund, große Unternehmen wie Facebook strenger zu behandeln als kleine (Bundeskartellamt wirft Facebook Datenmissbrauch vor, www.zeit.de 19.12.2017; Kartellamt übt scharfe Kritik an Facebook, SZ 20.12.2017, 1).

Bund

Geheimdienste überwachen mehr Telekommunikation

Das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) haben im Jahr 2016 gemäß einem Bericht des Parlamentari-

schen Kontrollgremiums (PKGr) des Bundestags insgesamt 261 „Individualmaßnahmen“ mit Eingriffen ins Fernmeldegeheimnis mit der Genehmigung der G-10-Kommission durchgeführt, 68 mehr als 2015. Die strategische Überwachung der Telekommunikation (TK) durch den BND läuft demgemäß oft leer. Die meisten Anordnungen gehen demnach auf das Konto der Staatsschützer. Auf das BfV entfielen 100 Einzelmaßnahmen im ersten und 124 im zweiten Halbjahr 2016. Die Tätigkeit des BND betrafen im vorigen Jahr insgesamt 33 Anordnungen. Der MAD führte parallel vier einschlägige Aktionen durch.

Gemäß dem Bericht bezogen sich beim BfV 139 Verfahren auf den Bereich Islamismus, 72 auf die Umtriebe anderer Geheimdienste und sieben auf Ausländerextremismus. Im Bereich Linksextremismus hat es keinen Fall und im Rechtsextremismus sechs Verfahren gegeben. Die BND-Maßnahmen beschäftigten sich ausschließlich mit dem Islamismus. Beim MAD hielten sich islamistischer Terrorismus und Nachrichtendienste jeweils mit 2 Verfahren die Waage.

Die Anzahl der Hauptbetroffenen belief sich 2016 auf insgesamt 817, während es im Vorjahr 658 waren. „Nebenher“ wurde die Telekommunikation von 634 Dritten (nach 437 im Jahr 2015) erfasst. Die Geheimdienste überwachten im Jahr 2016 3.747 Telekommunikationsanschlüsse, 2015 waren es 2838. Nachträglich informierten die Behörden 2016 nur 139 Personen, dass sie abgehört oder anderweitig ausspioniert wurden. 2015 erhielten noch 400 Betroffene eine entsprechende Mitteilung. Bei 33 Personen stellte die G-10-Kommission einstimmig fest, dass sie endgültig nicht informiert werden, hier lag die Zahl 2015 mit 188 deutlich höher. Betroffene können nur auf Basis einer entsprechenden Mitteilung gegen eine einschlägige Anordnung klagen.

13 Personen beschwerten sich im vorigen Jahr bei der G-10-Kommission, da sie einen ungerechtfertigten Eingriff in das in Artikel 10 Grundgesetz geschützte Post- und Telekommunikationsgeheimnis durch deutsche Geheimdienste befürchteten. Die Kontrolleure konnten aber in allen Fällen Entwarnung geben.

Das Volumen der „strategischen Fernmeldeaufklärung“ durfte der BND mit dem Plazet der G-10-Kommission nach einem deutlichen Rückgang 2015 im Zuge der Selektorenaffäre wieder erhöhen. Im Gefahrenbereich „Internationaler Terrorismus“ wurden 2016 im ersten Halbjahr 858 und im zweiten 1449 Suchbegriffe genehmigt, mit denen der Auslandsgeheimdienst die internationale Telekommunikation durchrastern durfte. 2015 waren es 858 Selektoren in der ersten und 904 in der zweiten Jahreshälfte. Im Filter des umstrittenen „Datenstaubsaugers“ des BND blieben dabei aber nur 34 Verkehre hängen, die als „nachrichtendienstlich relevant“ eingestuft wurden. 2015 schrieb der BND dies trotz der geringeren Zahl der Suchbegriffe noch 41 Vorgängen zu.

Im Bereich „Proliferation und konventionelle Rüstung“ ordneten die Kontrolleure im vorigen Jahr 179 zwischen Januar und Juni und 200 Suchbegriffe zwischen Juli und Dezember, 2015 lagen die Zahlen mit 271 beziehungsweise 239 Selektoren deutlich höher. Für eine „Relevanzprüfung“ qualifizierten sich 19 Verkehre im Vergleich zu nur elf 2015. Neu dazugekommen ist nach einer Gesetzesänderung der Gefahrensektor „Cyber“, wo der BND 2016 im ersten und zweiten Halbjahr mit je 1.144 Suchbegriffen operieren konnte. Herausgekommen ist dabei nichts: Der auswertende Fachbereich stufte keine Telekommunikationsverkehre als für ihn relevant ein. Nicht mehr aufgeschlüsselt wird, wie viele Telefonate, Mails, SMS oder Verbindungs- und Standortdaten sich zunächst für eine weitere Untersuchung qualifizierten.

Im Bereich der strategischen Maßnahmen, die viele Beobachtende als Massenüberwachung einschätzen, unterrichtete die G-10-Kommission gar keine Betroffenen. In einem Fall erfuhr das Gremium, dass Daten ohne eine gültige G-10-Anordnung erfasst worden seien und das Versehen erst im Nachgang festgestellt worden sei. Den entsprechenden Datensatz habe der BND „nicht weiter bearbeitet“ (Stefan Krempl, Deutlich mehr individuelle Überwachungen durch Verfassungsschutz und BND, www.heise.de 07.12.2017).

Bund

Drohneneinsatz beim G-20-Gipfel

Während des G-20-Gipfels in Hamburg setzten die Polizeien, das Bundeskriminalamt (BKA) und die Bundeswehr zahlreiche Drohnen in der Luft und unter Wasser ein. Gemäß einer als vertraulich eingestuften Aufstellung der Bundesregierung nutzte die Bundespolizei vom 03.-10.07.2017 Drohnen der Modelle „Inspire“, „Aladin“ und „Typhoon“, vor allem zur Kontrolle von Bahnstrecken und Grenzen. Kameras überflogen mehrmals Grenzübergänge nach Frankreich und in die Schweiz bei Weil am Rhein und nach Tschechien bei Waldhaus. Die Bundespolizei erklärte auf Anfrage, es seien nur „Übersichtsaufnahmen“ gemacht worden, um etwa entlang der grünen Grenze „einen unbemerkten Grenzübertritt von Personen oder Personengruppen zu verhindern“. Das BKA setzte Drohnen zur „Unterstützung von Durchsuchungsmaßnahmen im Sicherheitsbereich“ ein. Die Bundeswehr suchte mit Unterwasserdrohnen des Typs „Remus 100“ elfmal in der Elbe und der Alster nach versteckten Kampfmitteln, Brand- und Sprengvorrichtungen (Unbemannte Späher, Der Spiegel 51/2017, 17).

Bund

Anwaltspostfach beA geht wegen Sicherheitslücken nicht in Betrieb

Die Bundesrechtsanwaltskammer (BRAK) plante, mit Jahresbeginn 2018 das elektronische Anwaltspostfach einzuführen. Hierüber sollte der geschützte Mailverkehr zwischen Gerichten, Rechtsbeiständen und Behörden ermöglicht werden. Die Entwicklung des Projektes kostete die BRAK bisher 38 Mio. €. Nach zwei technischen Pannen in Folge bleibt das „besondere elektronische Anwaltspostfach“ (beA) erst einmal außer Betrieb. Eigentlich wären Rechtsanwälte seit Anfang 2018 rechtlich verpflichtet, ihr beA regelmäßig auf eingegangene Nachrichten zu überprüfen. Ab 2022 soll der Versand von Schriftsätzen und Dokumenten an

Gerichte nur noch über dieses Verfahren zulässig sein. Das Programm soll dank neuester Authentifizierungs- und Verschlüsselungstechniken garantieren, dass die Informationen wirklich nur von denen gelesen werden können, für die sie bestimmt sind. Vor Weihnachten 2017 zeigte der Chaos Computer Club (CCC) Darmstadt auf, dass das verwendete Sicherheitszertifikat nur unzureichenden Schutz bot. Markus Drenger vom CCC erklärte, die Programmierung von beA verstoße „vollkommen gegen den Stand der Technik und übliche Sicherheitsverfahren". Ein geheimes Zertifikat ließ sich frei von der Internetseite der BRAK herunterladen. 65.000 Anwender waren schon registriert.

Um den Zeitplan nicht zu gefährden, verschickte die BRAK daraufhin eilig an alle Verwendenden eine Anleitung, um ein neues Zertifikat zu installieren. Wer das versuchte, wurde von Windows ausdrücklich gewarnt und auf drohende Sicherheitsprobleme hingewiesen. Diese Meldung sollte man laut Anleitung der BRAK ignorieren. Tatsächlich barg das neue Zertifikat neue Gefahren. Nach der Installation hätten Hacker beA ausspionieren können; Passwörter oder Banking-Daten wären nicht mehr geschützt gewesen. Zahlreiche IT-Spezialisten warnten umgehend vor der Software. Daraufhin erklärte auch die BRAK, das Zertifikat sei unsicher und solle sofort wieder deinstalliert werden. Das gesamte System wurde noch vor Weihnachten vom Netz genommen.

Im neuen Jahr soll es erst einmal keine weiteren Schnellschüsse geben. Im Interesse von Sicherheit und Datenschutz will die Anwaltskammer die Anwendung erst freigeben, wenn die Vertraulichkeit der Übertragungen garantiert werden kann. Kritisiert wurde die BRAK, dass die Mängel zunächst als „vereinzelte Verbindungsprobleme" verharmlost wurden. Der Präsident des Deutschen Anwaltsvereins Ulrich Schellenberg forderte vom Bundesjustizministerium zur Installierungsverpflichtung eine „Klarstellung, dass das nicht gelten kann, solange beA offline ist" (Evers, Kommunikationssystem für Justiz und Anwälte bleibt offline, e-recht24.de 08.01.2018; Zgoll, Anwälte verpassen die Moderne, Kieler Nachrichten 06.01.2018, 1; Digitales Desaster, Der Spiegel 1/2018, 12).

Bund

AfD mit Microtargeting im Bundestagswahlkampf

Eine Untersuchung der Quadriga-Hochschule in Berlin ergab, dass die AfD teils mit juristisch heiklen Methoden im Wahlkampf zur Bundestagswahl 2017 mehr AnhängerInnen mobilisiert hat als die Konkurrenz. Bei der Auswertung der „digitalen Performance" der Bundestagsparteien ergab sich, dass es der AfD überdurchschnittlich gut gelang, Inhalte bei Twitter, Facebook und Instagram zu platzieren und weiterverbreiten zu lassen. Gemäß der Studie war die AfD „die einzige Partei, die auf datenschutzrechtlich bedenkliche Methoden zurückgriff". Die Rechtspopulisten haben demnach mittels Microtargeting Facebook-Nutzende in sieben Zielgruppen eingeteilt, darunter Mütter, Unternehmer, Arbeiter, Gewerkschafter. Diese bespielten sie gezielt mit bezahlter Werbung, insbesondere mit der Anti-Merkel-Webseite „Die Eidbrecherin". In der Studie wird für einen „Code of Conduct im Digital Campaigning" plädiert. Der digitale Wahlkampf sei längst integraler Teil von Wahlkämpfen. Im Trend lagen 2017 besonders Videos (Der Spiegel 50/2017, 23).

Bund

Mehr Transparenzpflichten bei Smartphone-Apps?

Die Justizminister von Nordrhein-Westfalen Peter Biesenbach (CDU) und von Baden-Württemberg Guido Wolf (CDU) wollen VerbraucherInnen vor einem unbemerkten Abgreifen ihrer Daten durch Smartphone-Apps besser schützen und dafür per Änderung des Bürgerliches Gesetzbuchs (BGB) eine Art „digitales Preisschild" einführen, das Auskunft über den Umfang des Datenabgriffs gibt. Wolf: „Ich finde es lohnenswert, dass wir diese Idee angehen und unterstütze sie ausdrücklich". Die Ressortchefs sind mit ihren Amtskollegen aus Bayern und Hessen im Gespräch über eine entsprechende Initiative im Bundesrat.

Eine Kennzeichnung könnte beim Download einer App leichter erkennbar machen, mit welchen persönlichen Daten der Nutzer die Software bezahlt. Nach einem entsprechenden Vorstoß von Peter Biesenbach aus Nordrhein-Westfalen sollen Programme wie die Jogger-App „Runtastic" oder der Chatdienst „WhatsApp" künftig mit prominent platzierten Hinweisen versehen werden – ähnlich einem Preisschild, das über den Umfang des Datenabgriffs informiert. Wolf: „Die Umsetzung wird sicher nicht leicht. Es werden sich beispielsweise komplexe europarechtliche Fragen stellen."

Nach den Plänen von Nordrhein-Westfalen sollen Anbieter der Apps dazu verpflichtet werden, an zentraler Stelle und schon vor Vertragsabschluss über sämtliche Daten zu informieren, auf die das jeweilige Programm zugreift. Per Klick soll der Kunde sein Einverständnis bestätigen müssen. Im Alltag ist es heute schon so, dass Apps vor dem Zugriff etwa auf Kamera, Fotos und Videos, Kontaktdaten oder Ortungsinformationen eine ausdrückliche Zustimmung der Nutzer verlangen (Justizminister will „Daten-Preisschild" für Gratis-Apps, www.t-online.de 13.11.2017; Datenidee aus Düsseldorf, SZ 09.11.2017, 6).

Bund

Telekom kündigt Sprachassistenten an

Die Deutsche Telekom will gemäß einer Präsentation am 13.11.2017 einen eigenen Sprachassistenten einführen. In Zusammenarbeit mit Partnern aus Forschung und Entwicklung erarbeitet das Unternehmen eine Sprachsteuerung für die Services der Telekom. Der Smart Speaker der Telekom soll im ersten Halbjahr 2018 auf dem deutschen Markt eingeführt werden. Der intelligente Sprachassistent soll Nutzern den Alltag erleichtern und die Angebote der Telekom auf den Zuruf „Hallo Magenta" steuern.

Das Unternehmen will mit einer engen Verzahnung mit hauseigenen Diensten wie dem Fernsehangebot EntertainTV und ihrer Router-Infrastruktur punkten. Der Lautsprecher soll sich damit di-

rekt verbinden, z. B. um Anrufe zu übernehmen. Der Konzern setzt dabei auf den Datenschutz: „Die Server befinden sich ausschließlich in Deutschland und unterliegen damit dem strengen deutschen Datenschutzrecht.“ Befehle sollen maximal 30 Tage gespeichert bleiben. Am Entwicklungsprozess des Smart Speakers sind Forschende des Fraunhofer Instituts für Digitale Medientechnologie aus Oldenburg maßgeblich beteiligt. Das Ergebnis soll ein kompaktes High-End-Stereo-Audiosystem mit zwei 42 Millimeter großen Lautsprechern, einer Ausgangsleistung von 25 Watt sowie einer Kombination aus vier hochempfindlichen Mikrofonen sein („Hallo Magenta“: Auch die Telekom plant smarten Lautsprecher, www.abendblatt.de 13.11.2017; „Hallo Magenta“ – Telekom stellt smarten Lautsprecher vor und setzt auf Datenschutz, www.4kfilme.de 15.11.2017).

Bundesweit

OpenSCHUFA will Scoring-Logik erkunden

Im Crowdfunding-Projekt OpenSCHUFA soll ermittelt werden, mit welchen Methoden die Scoringfirma Schufa Bonitäten ermittelt. Die Macher bitten hierfür auf der Plattform Startnext sowohl um Geld- als auch um Datenspenden. Bei dem Projekt soll festgestellt werden, ob die Ermittlung der Schufa-Scores, die z. B. beim Abschluss von Mobilfunk- oder Mietverträgen herangezogen werden, „systematische Fehler“ beinhalten. Es gibt Hinweise, dass die Schufa teilweise unvollständige Daten verwendet. Von mehreren hunderttausend Menschen sollen falsche Negativmerkmale gespeichert sein, die ihre Kreditwürdigkeit ruinierten. An Bord sind bei dem Projekt die Organisation Algorithmwatch und der Verein Open Knowledge Foundation Deutschland. Als Medienpartner wird das Nachrichtenmagazin „Der Spiegel“ genannt.

Gemäß eigenen Angaben speichert die Schufa 864 Millionen positive und negative Daten zu 67,5 Millionen natürlichen Personen und 5,3 Millionen Unternehmen. Wie aus den Daten der Bonitätsscore errechnet wird, muss das Unternehmen nicht offenlegen. Laut einem BGH-Urteil vom 28.01.2014 sind diese Verfahren ein schützenswertes Betriebsgeheimnis (DANA 2014, 47). Privatpersonen können einmal pro Jahr eine kostenlose schriftliche Auskunft über sich von der Schufa einholen. Die Projektmacher erbitten als Datengrundlage für ihr Vorhaben Selbstauskünfte von Betroffenen und verweisen auf die Seite selbstauskunft.net zur Einholung der Schufa-Daten. Dazu sollten UnterstützerInnen auch freiwillig noch personenbezogene Daten wie Alter, Geschlecht und Wohnort angeben. Zunächst soll aber erst eine Open-Source-Software entwickelt werden, mit der die Datenspenden automatisiert angenommen und verarbeitet werden können. Teil der Entwicklungsarbeit soll auch eine entsprechende Website sein, die UnterstützerInnen eine datenschutzfreundliche Übertragung ermöglicht, sowie eine sichere Datenhaltung.

Die Schufa hält nichts von dem Vorhaben. Die Kampagne sei „irreführend und gegen Sicherheit und Datenschutz in Deutschland“. Die Schufa sei intensiv reguliert und gegenüber Behörden und Aufsichten transparent; sie lege dem hessischen Datenschutzbeauftragten regelmäßig Rechenschaft ab. Zudem erfülle das Unternehmen eine wichtige Rolle im Wirtschaftsleben. Abgesehen davon warnt die Auskunftei auch vor Betrug und Missbrauch, denen durch ein Offenlegen der Scoreformel Vorschub geleistet werde: „Denn wer, wenn nicht derjenige, der seinen Score manipulativ verbessern möchte, sollte ein Interesse daran haben, die Details eines wissenschaftlich anerkannten und in der Praxis bewährten Berechnungsverfahrens zu kennen?“. Zudem warnt das Unternehmen potenzielle Unterstützende davor, sensible Daten wie ihre Selbstauskünfte an Dritte weiterzugeben, wenn nicht klar sei, inwieweit für die Sicherheit der Daten gesorgt werde. Für die Schufa könnte die Aktion einer interessengeleitete Kampagne sein, da Algorithmwatch von der Bertelsmann-Stiftung unterstützt wird. Zum Bertelsmann-Konzern gehört mit Arvato Infoscore ein eigenes Scoring-Unternehmen, das genau wie andere Schufa-Konkurrenten nicht Gegenstand des Projekts sei.

Arne Semsrott, Mit-Initiator von OpenSCHUFA, betonte auf Anfrage, dass die gespendeten Daten anonymisiert verarbeitet würden. Die Auflösung der Daten solle keinen Rückschluss auf Personen ermöglichen. Das Projekt wolle für eine Ende-zu-Ende-verschlüsselte Übertragungsmöglichkeit sorgen, die Speicherung soll ebenfalls verschlüsselt erfolgen. Zentral sei die Haupttabelle mit den Wahrscheinlichkeitswerten für verschiedene Branchen, alle weiteren Daten können Unterstützer freiwillig dazugeben. Die Schufa habe man als erstes ausgewählt habe, weil sie Marktführer und bekanntester Anbieter sei. Die entwickelte Software solle sich aber idealerweise auf Verfahren anderer Scoring-Dienstleister anwenden lassen: „Alle Scoring-Agenturen müssen transparenter werden.“ Unklar ist, weshalb die Kampagne nicht dahin läuft, von den Unternehmen direkt mehr Klarheit über die verwendeten Algorithmen einzufordern. Es dürfte fraglich sein, ob mit der Methode wirklich aussagekräftige Erkenntnisse erlangt werden können (Kannenberg, OpenSCHUFA: Projekt will Scoring-Methoden rekonstruieren, www.heise.de 15.02.2018).

Bundesweit

Auskunftsbereitschaft von Wohnungssuchenden gehorcht der Not

Die Mietpreise und die Wohnungsnot in den Ballungsräumen in Deutschland sind immer wieder ein Aufregerthema. Wegen der Wohnungsnot geben viele MieterInnen ihre Daten früh preis, ohne zu wissen, ob sie die Wohnung bekommen. Eine Umfrage des Meinungsforschungsinstituts YouGov ergab, dass sich gut die Hälfte der Befragten bereit zeigte, dem Vermieter schon vor einer Wohnungsbesichtigung die jüngste Einkommensbescheinigung vorzulegen. Ein Empfehlungsschreiben oder eine Zahlungsbestätigung vom bisherigen Vermieter würde ebenfalls die Hälfte der Befragten übergeben, noch bevor sie die Wohnung gesehen haben.

Eine solche Praxis ist jedoch datenschutzwidrig. Eine Broschüre des sogenannten Düsseldorfer Kreises, dem Kreis

der obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland, führt aus, dass der Vermieter zwar konkrete Gehaltsnachweise wie etwa einen – teilweise geschwärzten – Kontoauszug verlangen kann, aber erst, wenn er sich schon für einen Bewerber entschieden hat.

Wenige Probleme haben die Befragten damit, Daten über Alter, Haustiere und den Familienstand abzugeben, ohne zu wissen, ob die Wohnung nach einer Besichtigung überhaupt infrage kommt. Am schwersten tun sie sich mit der Schufa-Auskunft über die finanzielle Zuverlässigkeit: Mit 45% war der Anteil derjenigen, die diese schon früh übermitteln würden, geringer als bei vielen anderen Daten. Menschen in Ostdeutschland zeigten sich in manchen Bereichen vorsichtiger: So waren sie seltener als Westdeutsche bereit, Fragen nach Alter, Familienstand, Kindern und dem Rauchen früh zu beantworten.

40% der Leute gaben in der repräsentativen, online durchgeführten Umfrage an, dass zu viele Informationen vor einer Besichtigung verlangt würden. Die Mehrheit allerdings sah das weniger kritisch: 37% meinten, die Zahl der Fragen an die möglichen Mieter sei „genau richtig", 6% fanden, es würden noch zu wenig Informationen verlangt (Datenschutz auf dem Mietmarkt: Informationen werden zu früh preisgegeben, www.tz.de 08.12.2017).

Kirchen

Sieben Katholische Bistümer benennen Datenschutzbeauftragte

Die (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier haben eine gemeinsame Datenschutzstelle errichtet. Sitz dieser überdiözesanen Aufsichtsstelle im Datenschutz für alle kirchlichen Einrichtungen der beteiligten Diözesen ist Frankfurt am Main. Geleitet wird die neue Einrichtung seit 01.01.2018 von Ursula Becker-Rathmair. Die Juristin ist gemeinsame Diözesandatenschutzbeauftragte und seit vielen Jahren in diesem Bereich tätig. Vor ihrem Wechsel nach Frankfurt leitete die gebürtige Kölnerin fast 27 Jahre die Rechtsabteilung im Bistum Erfurt und war als Justiziarin mit allen Rechtsgebieten, die eine Diözese betreffen, befasst. Ab 1992 war sie im Bistum Erfurt zudem Diözesan-Datenschutzbeauftragte. Mit der Einrichtung der gemeinsamen Datenschutzstelle kommen die beteiligten (Erz-)Diözesen den Verpflichtungen des künftigen europäischen Datenschutzrechtes nach, wonach ein unabhängiger Datenschutz gewährleistet werden muss.

Kontakt: Datenschutzstelle der (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier, Haus am Dom, Domplatz 3, 60311 Frankfurt, Tel.: 069-8008718-0, E-Mail: u.becker-rathmaier@kdsz-ffm.de (Datenschutz über die Bistumsgrenzen hinaus, www.bistum-trier.de 04.01.2018).

Bayern

Änderungen des Polizei- und Datenschutzrechts

Die bayerische Staatsregierung beschloss am 28.11.2017 eine Änderung des bayerischen Polizeirechts sowie Änderung des Landesdatenschutzrechts, mit denen Vorgaben der Europäischen Union (EU) und des Bundesverfassungsgerichts umgesetzt werden sollen. Danach soll die Polizei mehr Befugnisse im Kampf gegen Terrorismus und Internetkriminalität erhalten. Bei einem drohenden Terroranschlag soll die bayerische Polizei DNA-Spuren künftig nicht nur zur Strafverfolgung, sondern auch zur Gefahrenabwehr sichern und auswerten dürfen, so Innenminister Joachim Herrmann (CSU), „wenn die Polizei zum Beispiel die Werkstatt eines potenziellen Bombenbauers aushebt, ohne diesen aber am Tatort anzutreffen". Rechtlich war dies bisher nicht möglich. Die Ermittler dürften dann mit den DNA-Spuren Geschlecht, Hautfarbe und ethnische Herkunft des unbekannten Bombenbauers ermitteln.

Wenn Hacker im Internet mit Viren und Trojanern Bitcoins und anderes virtuelles Geld erpressen, soll die bayerische Polizei das Geld künftig „zunächst sichern und den wahren Eigentümer ermitteln, unabhängig von einem Strafverfahren". Polizisten sollten auch häufiger Bodycams tragen. Das helfe, so Herrmann, zum Beispiel Opfern häuslicher Gewalt. Randalierende Hooligans, die einen Polizeieinsatz verursachen, könnten künftig für die Kosten herangezogen werden (Polizei bekommt mehr Rechte bei der Terrorabwehr, www.welt.de 28.11.2017, s.o. S.11).

Bayern

LKA plant verstärkte automatisierte Gesichtserkennung

Seit knapp zehn Jahren nutzt das Landeskriminalamt (LKA) des Freistaates Bayern biometrische Gesichtserkennung, um Tatverdächtige zu ermitteln. Das Innenministerium des Landes will die Fahndungsmethode ausbauen. Nach dem Willen von Innenminister Joachim Herrmann (CSU) sollen mit dieser Methode künftig noch mehr Tatverdächtige erkannt werden. Im Jahr 2017 wurden durch biometrische Gesichtserkennungen Jahr ca. 100 Tatverdächtige von der Polizei ermittelt, zehn Mal mehr als vor sieben Jahren, kurz nach der Einführung. Ein Fall ist Bernhard Egger vom LKA in besonderer Erinnerung, der Diebstahl eines iPads, der letzten Endes durch die Biometrie geklärt wurde: „Der Geschädigte kam nach ein paar Wochen zu uns, mit Bildern, die in seine Cloud hochgeladen waren von einer Hochzeit – das war nicht seine Hochzeit. Und wir haben dann diese Bilder mit der Gesichtserkennung analysiert und konnten feststellen, dass der Bräutigam dann später der vermeintliche Täter oder Mittäter war und konnten ihn so identifizieren." Offen bleibt, ob den Verdächtigen im Nachhinein auch wirklich immer eine Straftat nachgewiesen werden konnte.

Das LKA nutzt seit 2008 ein Gesichtserkennungssystem des Bundeskriminalamts (BKA) zur Identifizierung von unbekannten Straftätern. Dabei werden Bild- und Videodaten von potenziellen Straftätern per Software mit der Datenbank Inpol abgeglichen, einem länderübergreifenden Informationssystem der Polizeien. Die Bilder werden automatisiert erfasst, analysiert und abgegli-

chen. Florian Gallwitz von der Technischen Hochschule Nürnberg erläutert, dass dann ein Maß für die Ähnlichkeit von zwei Gesichtern festgelegt werden: „Man muss eine Software so programmieren, dass das gleiche Gesicht erkannt wird, egal, ob die Person beispielsweise eine Brille trägt, oder einen Bart, oder eine Mütze. Das macht man heutzutage mit künstlichen neuronalen Netzen mit vielen Millionen Parametern. Die technischen Verfahren funktionieren schon verblüffend gut – besser, als der Mensch mehrere Fotos miteinander abgleichen könnte. Aber hundertprozentige Trefferquoten hat man nicht, man muss immer mit Fehlern rechnen".

Die Biometrie-Fahnder des LKA können mittlerweile auf ca. 5 Mio. Fotos von ca. 3,5 Mio. verurteilten StraftäterInnen zurückgreifen. Immer wieder werden Fotos von zunächst unbekannten Tatverdächtigen bereits bekannten Tätern zugeordnet. Innenminister Herrmann erläuterte: „Wir können wesentlich besser als bisher Personen, von denen wir ein Bild haben, deren Identität aber nicht bekannt ist, dadurch identifizieren, gerade wenn sie schon einmal auffällig geworden sind, wenn sie im Datenbestand des Landeskriminalamts oder anderer Polizeibehörden erfasst sind. Und deshalb haben wir bisher schon erhebliche Ermittlungserfolge, ich verspreche mir davon aber noch viel mehr in der Zukunft."

Bernhard Egger, Leitender Kriminaldirektor im LKA, beschreibt die Methode: „Es wird ein Algorithmus gebildet, der nach ganz bestimmten Merkmalen im Gesicht sucht. Das sind Merkmale, die unveränderlich sind, wie Abstände der Augen oder der Wangenknochen. Daraus wird dann ein Muster errechnet. Und dieses Muster wird in der Datenbank sozusagen als mathematischer Wert zu dem Bild hinterlegt." Nicht jedes Bild sei für einen biometrischen Abgleich geeignet. Bis jetzt müssen die Fotos direkt von vorne aufgenommen sein, doch seien die technischen Fortschritte absehbar: „Die Algorithmen werden immer besser, und man arbeitet jetzt schon an Algorithmen, die dreidimensional vermessen."

Die Bilder für die Fahndung nach StraftäterInnen stammen, so der Innenminister, insbesondere von der öffentlichen Videoüberwachung: „Wir haben sie in Zusammenarbeit mit den Kommunen in den letzten Jahren im U-Bahn-, S-Bahn-Bereich, in Bussen und Straßenbahnen ausgebaut. Und wir werden sie dort, wo es besonders viel Kriminalität gibt, an einzelnen Plätzen einzelner Städte weiter ausbauen. Wir denken nicht an den flächendeckenden Ausbau von Videoüberwachung beispielsweise in Innenstädten, wie man das in Großbritannien erleben kann."

Eine Videoüberwachung, die Passanten quasi live und im Vorbeigehen biometrisch erfasst, wird seit August 2017 in Berlin ein halbes Jahr lang getestet. Katharina Schulze, die sicherheitspolitische Sprecherin der Grünen im Bayerischen Landtag, erklärte dazu, dass nicht alles, was machbar ist, angewendet werden sollte: „Eine Sache ist klar: Es kann natürlich nicht dazu kommen, dass am Ende Bewegungsprofile von unbescholtenen Bürgerinnen und Bürgern im öffentlichen Raum erstellt werden. Und deswegen schauen wir Grünen besonders kritisch auf die intelligente Videoüberwachung, wo es ja jetzt die ersten Testläufe in Berlin gibt. Da müssen wir als Bürger und Demokraten natürlich immer genau hinschauen, wo in die Freiheit und wo auch in die Privatsphäre von uns allen zu tief eingegriffen wird" (Bayern will Gesichtserkennung als Fahndungsmaßnahme ausweiten, www.heise.de 01.12.2017; Pfeifer, Herrmann will Fahndung per Gesichtserkennung ausweiten, www.br.de 02.12.2017).

Bremen

Facebook-Einwilligungen weder freiwillig noch informiert

Die Einwilligung der Betroffenen gilt als die zentrale Legitimationsgrundlage für eine Verarbeitung personenbezogener Daten im Internet. Eine aktuelle interdisziplinäre Studie des Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen hat untersucht, ob Facebook-Nutzende tatsächlich „freiwillig, für den bestimmten Fall" und „in informierter Weise" in die verschiedenen Datenverarbeitungen einwilligen, wie dies gesetzlich vorgegeben ist.

Robert Rothmann, Gastwissenschaftler am IGMT und Studienautor, hat hierfür im Rahmen eines umfassenden Online-Survey 1.019 aktive Facebook-Nutzende befragt. Den TeilnehmerInnen wurde eine Reihe von besonders markanten Klauseln aus den Nutzungsbedingungen von Facebook vorgelegt, wobei jeweils gefragt wurde, ob die User wissen, dass sie eingewilligt haben (informierte und bewusste Einwilligung), und ob sie einwilligen würden, wenn sie die Wahl hätten (hypothetische Einwilligung).

Neben Themen wie der Klarnamenpflicht und dem Verzicht auf Löschung geteilter Informationen wurde auch die Einwilligung in die unbezahlte Nutzung von Name und Profilbild zur Aufwertung von Werbeanzeigen (Social Ads) sowie die Analyse persönlicher Informationen für Studien und Produktentwicklung (Big Data Analytics) adressiert. Auch die Weiterleitung persönlicher Daten in die USA (Privacy Shield) und die Einwilligung in den behördlichen Zugriff auf die Daten wurden abgefragt.

99% der Befragten wussten nicht, dass sie in alle ihnen vorgelegten Klauseln eingewilligt hatten. Lediglich 3% hätten in alle vorgelegten Klauseln eingewilligt, wenn sie wirklich die Wahl gehabt hätten. Vertiefende qualitative Analysen verdeutlichen, dass die inhaltliche Konfrontation mit den Bestimmungen unter den Betroffenen weitgehend Kritik und Empörung auslöst. Rothmann schließt daraus: „Die Ergebnisse zeigen, dass die freiwillige Nutzung von Facebook nicht mit der Einwilligung in die daran gekoppelten Datenverarbeitungen gleichzusetzen ist." Facebook zu nutzen bedeute gerade nicht, zugleich sämtlichen Vertragsinhalten und Datenverarbeitungsprozessen pauschal zuzustimmen. Die repräsentativen Daten belegten, dass für durchschnittliche VerbraucherInnen im Fall von Facebook (auf subjektiver Tatbestandsebene) keine informierte Einwilligung vorliegt.

Die Auffassung von Facebook und einiger JuristInnen, der Akt der Registrierung bei Facebook können als formgültige Erklärung und Einwilligung interpretiert werden, sehen die Studienverfasser widerlegt. KonsumentInnen, die sich bei einem Social Media Dienst

anmelden, dem umfangreiche AGB zu Grunde liegen, deren Kenntnisnahme ökonomisch irrational und deren Verständnis für juristische Laien praktisch unmöglich ist, wird quasi unterstellt, mit den diversen Aktivitäten und Datenverarbeitungen einverstanden zu sein.

Die Einwilligung erweise sich somit als dogmatische Fiktion. Diese schütze die Unternehmen („Vertrauensschutz" des Erklärungsempfängers) und ermögliche eine datenschutzrechtliche Übervorteilung der VerbraucherInnen im digitalen Massengeschäft. Rothmann spricht von einer vertragsrechtlich gestützten Erosion der Privatsphäre (IGMT, PE 22.02.2018, Datenschutzrechtliche Einwilligung ist Fiktion: Interdisziplinärer Facebook-Survey liefert umfassenden Einblick).

Hamburg

Große Öffentlichkeitsfahndung nach G-20-Gewaltverdächtigen

Mit teilweise hoch aufgelösten Einzelfotos und Videosequenzen sucht die Hamburger Polizei u. a. auf der Internetseite polizei.hamburg.de nach 104 mutmaßlichen G-20-TäterInnen – und bittet öffentlich um Mithilfe. Oberstaatsanwalt Michael Elsner erläuterte, dass es in allen Fällen um „Straftaten von erheblicher Bedeutung" gehe, etwa um schweren Landfriedensbruch, Brandstiftung oder schwere Körperverletzung. Gestartet wurde damit einer der größten Fahndungsaufrufe der bundesdeutschen Rechtsgeschichte. Geworben wurde dafür ab dem 18.12.2017 mit verstörenden Filmszenen, etwa Bildern von Randalierern, die während des G-20-Gipfels im Juli 2017 in der Hansestadt wüteten: Flaschen und Böller flogen da, Chaoten verwüsteten einen Supermarkt. Ein Vermummter schmetterte einen Stein auf den behelmten Kopf einer Beamtin, die zu Boden ging.

- Die Fahndungsaktion

Die Aufnahmen sind in verschiedene Themenkomplexe aufgeteilt: Plünderungen (44 Gesuchte), Stein- und Flaschenwürfe (17), Straftaten in den Straßen Elbchaussee (5), Rodenbarg (25) und beim Aufmarsch „G20 – not welcome!" (13). Polizeisprecher Timo Zill nannte die Öffentlichkeitsfahndung eine „wichtige Etappe" auf dem Weg, G-20-Täter dingfest zu machen. Bei jedem Beschuldigten lägen eine oder mehrere Taten vor, die man ihm konkret vorwerfe. „Wir fragen die Bevölkerung: ‚Wer kann den Fotos und Gesichtern eine Identität geben?'" Die Soko „Schwarzer Block" bearbeitet laut Zill mehr als zwölf Terabyte Bilddateien. Insgesamt verfolgen in der Ermittlungsgruppe 163 PolizistInnen 3.340 Fälle. Die Polizei schätzt, dass vom 06.-08.07.2017 5.000 bis 6.000 vor allem männliche Täter aktiv gewesen sind. Doch auch einige Frauen werden gesucht. Auffällig ist etwa eine junge blonde Frau mit einem bauchfreien Top und rot-weißen Turnschuhen, die unter dem Tatkomplex Stein- und Flaschenwurf aufgeführt wird. Zill kündigte bereits Folgeaufrufe an: „Es wird weitere Fahndungen geben, weil wir erhebliches Beweismaterial haben, das noch ausgewertet wird." Die Bilder des Fahndungsaufrufs der Hamburger Ermittler stammen aus Polizeikameras, aus öffentlichen Überwachungskameras und aus privaten Videos. Die Polizei hatte auch BürgerInnen und JournalistInnen gebeten, Bildmaterial zur Verfügung zu stellen. Die Presse stellte teilweise ihre nicht veröffentlichten Bilder zur Verfügung, andere Medien verweigerten das Material aber mit dem Argument des Quellenschutzes. Welche Quelle jedes einzelne Bild hat, wurde nicht offengelegt.

Der Fahndungsaufruf führte schon kurzfristig zu Rückmeldungen. Schon am ersten Tag nach dem Aufruf gingen 80 Hinweise bei der Polizei ein; nach drei Tagen 187, bis zum Jahresende 2017 228. Nach drei Tagen waren sechs der insgesamt 104 Gesuchten identifiziert, darunter auch eine 17jährige Jugendliche – die blonde Frau mit dem bauchfreien Top. Zum Jahresende 2017 waren insgesamt 15 Verdächtige identifiziert. Ein Mann meldete sich, bei der – präsentierten – Plünderung eines Supermarkts anwesend gewesen zu sein, aber nicht geplündert, sondern als YouTuber gefilmt zu haben. Ende Januar 2018 waren 23 Gesuchte identifiziert. Zehn von ihnen sollen Steine oder Flaschen auf Beamte geworfen, neun sich an Plünderungen beteiligt haben. Einer der Identifizierten steht im Verdacht, sich an Ausschreitungen am Rande der Demonstration „G20 not welcome" beteiligt zu haben. Bis dahin hatte die Soko keinen der Gesuchten aus den Tatkomplexen Rondenbarg (25 Tatverdächtige) und Elbchaussee (5) identifizieren können. An der Elbchaussee hatten am Morgen des 07.07.2017 rund 220 Vermummte Autos angezündet und einen Hubschrauber mit Pyrotechnik beschossen. In der Straße Rondenbarg in Hamburg-Bahrenfeld hatte nach Polizeiangaben kurz zuvor eine größere Gruppe von vermummten und uniformierten Personen Beamte mit Steinen und Böllern beworfen.

Anfang Februar 2018 teilte Innensenator Andy Grote (SPD) mit, dass die öffentliche Fahndung nach Verdächtigen auf andere Staaten ausgeweitet werde: „Wir arbeiten derzeit daran, mit entsprechendem Bildmaterial auch im europäischen Ausland öffentlich zu fahnden." Zuvor waren die Bilder von mutmaßlichen Randalierern und Plünderern routinemäßig schon intern mit Polizeibehörden anderer EU-Staaten ausgetauscht.

- Öffentlichkeitsfahndung

Eine Öffentlichkeitsfahndung ist das letzte Mittel von Polizei und Staatsanwaltschaft. Dafür muss laut Gesetz nicht nur eine Straftat von erheblicher Bedeutung vorliegen. Es müssen auch alle anderen Ermittlungsschritte erfolglos geblieben sein. Kriminalpsychologe Rudolf Egg erläutert: „Es gilt bei einer Öffentlichkeitsfahndung im besonderen Maße, die Persönlichkeitsrechte gegen das Strafverfolgungsinteresse abzuwägen. Dass zunächst Verdächtige sich später als unschuldig erweisen, kommt häufig vor. Im Fall einer Öffentlichkeitsfahndung aber ist dann das Foto des Betroffenen in der Welt. Das kann schwere Folgen haben, etwa den Verlust des Arbeitsplatzes und die Ächtung im persönlichen Umfeld." Egg warnt davor, eine Öffentlichkeitsfahndung „zu oft" zu machen: „Die Aufklärung von Straftaten ist kein Volkssport, sondern Aufgabe von Polizei und Justiz." Der Gipfel sei für die Hamburger Polizei „eine Blamage" gewesen. „Deshalb versucht man, wenigstens im Nachhinein, bei der Straf-

verfolgung alles richtig zu machen.“ Oberstaatsanwalt Elsner betonte, man habe nach den 104 Unbekannten mit internen Mitteln vergeblich gesucht. Erst danach habe man beim Amtsgericht Hamburg die öffentlichen Fahndungen beantragt. „Unterschiedliche Richter haben entsprechende Beschlüsse erlassen.“

- Reaktionen

Linksextreme reagierten auf die Öffentlichkeitsfahndung damit, dass sie Fotos von 54 Polizisten veröffentlichten, was wiederum Empörung und Entsetzen bei Polizeigewerkschaften auslöste. Auf der Seite indymedia.org heißt es, die Berliner Polizisten hätten an Häuserräumungen im Berliner Stadtteil Friedrichshain teilgenommen: „Wir freuen uns über Hinweise, wo sie wohnen oder privat anzutreffen sind. Neben der Teilnahme an der Räumung können sie bedenkenlos für die Gewalt der drei Wochen der Belagerung verantwortlich gemacht werden.“ Die Gewerkschaft der Polizei (GdP) reagierte auf diesen „Fahndungsaufruf“: „Das muss strafrechtliche und politische Konsequenzen haben.“ Und Stephan Mayer (CSU), innenpolitischer Sprecher der Unionsfraktion im Bundestag, schimpfte über „einen unsäglichen Vorgang“. Der Staatsschutz nahm Ermittlungen auf. Die Bundesdatenschutzbeauftragte Andrea Voßhoff (CDU) erklärte: „Für die Veröffentlichung der Bilder von Polizeibeamten auf Indymedia gibt es keine Rechtsgrundlage. Aus Sicht des Datenschutzes liegt eine erhebliche Verletzung des Persönlichkeitsrechts der Betroffenen vor. Es steht allen Betroffenen frei, strafrechtliche und zivilrechtliche Maßnahmen einzuleiten.“

Die innenpolitische Sprecherin der Linksfraktion in der Hamburger Bürgerschaft, Christiane Schneider, warf der Polizei „Stimmungsmache“ vor. Die Fahndung sei unverhältnismäßig. Die Polizei sage in vielen Fällen nicht, wo die Gesuchten in den Filmen auftauchen. Dadurch würden die Leute „pauschal für die schwere Randale verantwortlich gemacht“, die es ohne Zweifel gegeben habe. Schneider unterstellte der Polizei, sie wolle sämtliche Proteste gegen G-20 als gewalttätig darstellen. Bei der Demo „G20 – not welcome“ etwa seien mehr als 70.000 Menschen mitgelaufen. Nur aus einer Gruppe von 200 Leuten heraus habe es Gewalt gegeben, nach einigen dieser Personen werde nun gesucht. Das Fehlverhalten dieser Leute diskreditiere aber nicht die gesamte Veranstaltung. Ähnlich kommentierte Heribert Prantl in der Süddeutschen Zeitung: „Die Öffentlichkeitsfahndung nach G-20-Tätern ist ein Exzess.“ Er fragte danach, wie sich diese „Art Massenscreening“ bzw. „gewaltige Schleppnetzfahndung“ mit der Unschuldsvermutung verträgt, zumal die Fotos der Betroffenen in der Welt bleiben, unabhängig davon, was die Ermittlungen ergeben. Und auch Konstantin von Notz von der grünen Bundestagsfraktion äußerte sich kritisch: „Man fragt sich, wo beginnt die Öffentlichkeitsarbeit der Polizei und wo endet die Fahndung. Ich erwarte, dass die Sicherheitsbehörden kühl und nüchtern ermitteln und nicht kampagnenartig zur Jagd blasen.“

Umgehend gingen drei Beschwerden beim Presserat ein, die sich gegen die „Krawall-Barbie“-Schlagzeile der Bildzeitung wendeten. Eine Sprecherin der Innenbehörde von Hamburg meinte: „Die Medien machen, was sie wollen.“ Der Kriminologe Bernd Maelicke hinterfragte gerade diese polizeiliche Veröffentlichung: „Wurde bei der richterlichen Freigabe dieses Fotos zur öffentlichen Fahndung berücksichtigt, dass es sich bei dieser verdächtigen Person um eine offensichtlich Jugendliche handelt, für die das Jugendstrafrecht gilt? Wurde der Schutzgedanke des Jugendstrafrechts im Interesse der Erziehung jugendlicher Angeklagter erkannt und geprüft?“

Innensenator Andy Grote lobte, dass die Öffentlichkeitsfahndung einen „weiteren Schritt zur Aufklärung“ darstellt. CSU-Landesgruppenchef im Bundestag Alexander Dobrindt kritisierte die Kritiker der Polizeiaktion: „Wer die Öffentlichkeitsfahndung für verfehlt hält, stellt offensichtlich den Täterschutz vor den Opferschutz“. Auch Hamburgs grüner Justizsenator Till Steffen verteidigte das Vorgehen: „Die Staatsanwaltschaft hat sich vom Vorliegen der rechtlichen Anforderungen nach sorgfältiger Prüfung überzeugt und das Amtsgericht hat diese Einschätzung bestätigt.“ Die SPD-Bundestagsfraktion, die vor möglichen Koalitionsverhandlungen mit der Union um ihr sozialdemokratisches Profil rang, ließ ihren sicherheitspolitischen Sprecher Burkhard Lischka ausrichten, „aus terminlichen Gründen“ können er dazu nichts sagen.

- Datenschutz

Der Hamburgische Datenschutzbeauftragte Johannes Caspar hält die von der Soko „Schwarzer Block“ gestartete massenhafte Öffentlichkeitsfahndung nach Gewalttätern im Rahmen der G20-Krawalle „gerade im Internetzeitalter“ für „nicht geeignet“. Dies schieße weit übers Ziel hinaus: „Die Gewalt beim G20-Gipfel ist schockierend. Das zeigen die nun veröffentlichten Bilder erneut. Die Öffentlichkeitsfahndung stellt gleichwohl ein massiv-eingriffsintensives Instrument dar, das hier in einem bislang kaum vergleichbaren Ausmaß eingesetzt wird.“ Personen, nach denen mit Hilfe öffentlicher Medien gefahndet werde, würden „in ihrem persönlichen Umfeld vor der Allgemeinheit bloßgestellt“, was „begleitend auch ein sanktionierenden Charakter“ habe. Gerade im Internetzeitalter sei eine Öffentlichkeitsfahndung nach mehr als 100 Personen fragwürdig, „auch wenn die strafprozessuale Legalität jedes einzelnen Falles durch die individuelle richterliche Anordnung jeweils verbürgt sein mag“. „Die Vorabveröffentlichung von einigen Personen ohne richterliche Anordnung“ im Boulevardblatt „Bild“ Ende November sei eindeutig rechtswidrig gewesen sei. Zumindest fragwürdig sei auch die Praxis der Öffentlichkeitsfahndung über Facebook. Schon der Betrieb einer behördlichen Fanpage auf der Plattform erscheine „rechtlich bedenklich“, nachdem ein Generalanwalt des Europäischen Gerichtshof (EuGH) jüngst festgestellt habe, dass solche Anbieter „datenschutzrechtlich verantwortlich sind und hierauf das nationale Recht anwendbar ist“ (Siemens, Letzte Hoffnung Öffentlichkeit, www.spiegel.de 18.12.2017; Gesicht der Gewalt, SZ 19.12.2017, 7; Krempl, Datenschützer tadelt Hamburger Polizei für massenhafte Internetfahndung nach G20-Randalierern, www.heise.de 19.12.2017; Prantl, Aktion Halali, SZ 20.12.2017, 4; Hahn, Galerie mit Brandstiftern und Plünderern, SZ 20.12.2017,

6; Neue Kritik an G-20-Fotofahndung, SZ 22.12.2017, 6; Baumgärtner/Großbongart/Kühn, Brille, Bart, Glatze, Der Spiegel 52/2017, 43; Majewsky, 15 Verdächtige identifiziert, Kieler Nachrichten 30.12.2017, 14; Hamburger Fotofahndung – 20 mutmaßliche G20-Gewalttäter ermittelt, www.heise.de 20.01.2018; Foto-Fahndung im Ausland, SZ 02./03.02.2018, 7).

Rheinland-Pfalz

Keine Transparenz über Speicherung gewaltbereiter Fußballfans

Von der Polizei beobachtete Fußballfans sollten aus Sicht des rheinland-pfälzischen Landesdatenschutzbeauftragten Dieter Kugelmann von der Aufnahme in eine besondere Datei benachrichtigt werden. Kugelmann ist dazu im Gespräch mit dem Innenministerium. Auch bei der sogenannten SKB-Datei für „Szenekundige Beamte" (SKB) sollte es eine Benachrichtigungspflicht für Betroffene geben: „Bei diesen Eintragungen ist eine Benachrichtigung bislang zwar nicht gesetzlich vorgeschrieben, aus unserer Sicht aber sinnvoll." Ein Betroffener sollte die Gelegenheit haben, sich gegen die Aufnahme in die Datei wehren zu können. Auch nach der neuen EU-Datenschutzrichtlinie für Polizei und Justiz spreche sehr viel dafür, dass eine Benachrichtigung erforderlich sei (vgl. DANA 1/2017, 47 f.; 66).

Im Anschluss an eine Anfrage an die Landesregierung zur SKB-Datei kritisierte die Parlamentarische Geschäftsführerin der Grünen-Fraktion, Pia Schellhammer: „Diese Praxis ist für viele Fußballfans intransparent und wird zurecht bis Mitte des Jahres einer Evaluation unterzogen." Der sportpolitische Sprecher Daniel Köbler ergänzte, der Mehrwert einer Geheimhaltung sei für ihn nicht ersichtlich: „Es könnte sogar einen präventiven Nutzen haben, wenn man weiß, dass man schon im Visier der Polizei ist." Präventive Maßnahmen gegen Gewalt bei Fußballspielen seien erforderlich, müssten aber zielgerichtet sein und im Einklang mit den Bürgerrechten stehen.

Im Unterschied zur bundesweiten Verbunddatei „Gewalttäter Sport" wird die SKB-Datei nur von einem geschlossenen Kreis einzelner Beamter genutzt. In ihr sind nach Angaben des Innenministeriums zurzeit rund 220 Personen verzeichnet. Die Datei „Gewalttäter Sport" enthält rund 350 Personen, die Vereinen in Rheinland-Pfalz zugerechnet werden (Datenschützer: Fans sollen von Eintrag in Datei erfahren, www.allgemeine-zeitung.de 05.01.2018).

Schleswig-Holstein

Hausherr außer Haus – Alexa feiert

Während Oliver H. aus Pinneberg am 03.11.2017 auf der Hamburger Reeperbahn, so seine eigene Darstellung, „ganz entspannt ein Kaltgetränk" zu sich nahm, nutzte Alexa, die sich bis dahin durch ausgesprochenes Wohlverhalten ausgezeichnet hatte, die Abwesenheit des Hausherrn, um in der Wohnung im sechsten Stock eine ausschweifende Party zu veranstalten. Um 01.42 Uhr, so der Polizeibericht, hatte eine Nachbarin Alarm geschlagen, weil aus H.s Wohnung in voller Lautstärke Musik dröhnte. Da selbst auf lang anhaltendes Klingeln und Klopfen niemand reagierte, ließen sich die Beamten von einem Schlüsseldienst die Tür öffnen.

Alexa ist kein aufmüpfiger Teenager, sondern das auf künstlicher Intelligenz (KI) basierende Sprachsystem von Amazon, das in der für gut 100 € erhältlichen Lautsprecher-Box Echo steckt. Mit Echo und Alexa, so deren Anbieter Amazon, wird die Wohnung zum von der menschlichen Stimme gesteuerten Smart Home, so dass auf mündlichen Befehl das Licht, der Fernseher oder das Babyphone ein- oder ausgeschaltet werden. Sind das Türschloss und der Kühlschrank mit vernetzter Technologie ausgestattet, so kann Alexa auch kontrollieren, ob die Haustür abgeschlossen oder noch genug Milch da ist.

H. versicherte, dass es keine menschliche Stimme gab, die einen Befehl hätte formulieren können. Niemand habe sich in der Wohnung aufgehalten. Auch der Musikstreaming-Dienst auf seinem Handy habe seines Wissens nach keine Verbindung zur Amazon-Box gehabt. Auch sei kein Fenster gekippt gewesen, so dass eventuell jemand von außerhalb des Hauses das Gerät in Gang gesetzt haben könnte.

Die Panne von Pinneberg erinnert an andere Fehlleistungen sog. KI mit zum Teil gravierende Folgen. Im Jahr 2015 etwa identifizierte eine vermeintlich smarte Bilderkennungssoftware von Google zwei schwarzhäutige Menschen als Gorillas. 2016 starb ein Mann, weil der durch KI gesteuerte Autopilot eines Tesla-Sportwagens einen LKW mit einem über der Fahrbahn hängenden Verkehrsschild verwechselt hatte. Hinsichtlich der Datensicherheit ist Alexa problematisch, da z. B. sämtliche Sprachbefehle an Alexa in der Amazon-Cloud gespeichert werden und der Lautsprecher ständig den Raum abhört, um sich auf ein bestimmtes Signalwort hin in Gang setzen zu können.

Auf der Suche nach einer Erklärung konsultierte der frustrierte Nutzer Alexa selbst. Doch das Sprachsystem erwiderte nur: „Ich habe leider keine Antwort auf deine Frage gefunden." H. entschied sich daraufhin, das Gerät an den Hersteller zurückzuschicken, was Amazon ohne Umstände akzeptierte. Nach einigen Tagen legte Amazon eine Stellungnahme vor, wonach man gemeinsam mit dem Kunden „den Grund für den Vorfall identifiziert" habe. Das Lautsprechersystem Echo sei durch „Fernzugriff aktiviert und auf maximale Lautstärke gestellt" worden. Verantwortlich sei, offenbar entgegen dem, was H. zunächst sagte, „die kundeneigene Music-Streaming-App eines Drittanbieters". Amazon legt Wert auf die Feststellung, dass Alexa keinen Fehler gemacht habe. Trotzdem werde das Unternehmen die durch den Polizeieinsatz verursachten Kosten erstatten (Klasen, Alexa allein zu Haus, SZ 07.11.2017, 21; Koch, Amazon übernimmt Kosten für nächtlichen Polizeieinsatz, www.welt.de 09.11.2017).

Datenschutznachrichten aus dem Ausland

Weltweit

UN-Sicherheitsrat fordert zur PNR-Sammlung auf

Die Vereinten Nationen (United Nations – UN) wollen im Kampf gegen den Terrorismus die Überwachung von Reisenden deutlich ausbauen. Gemäß einer Resolution des UN-Sicherheitsrats vom 21.12.2017 sollen alle Mitgliedstaaten Systeme entwickeln und einsetzen, mit denen sie Flugpassagierdaten in Form von Passenger Name Records (PNR) sowie die weniger detailreichen Advanced Passenger Information (API) verarbeiten und analysieren können. Die 193 beteiligten Nationen werden zudem angehalten, biometrische Daten wie Fingerabdrücke oder Gesichtsbilder zu sammeln und etwa mit Verfahren zur automatischen Gesichtserkennung auszuwerten. Ziel soll es sein, „verantwortungsvoll und ordnungsgemäß entsprechend nationaler Gesetze und internationaler Menschenrechtsvorgaben" Terroristen einschließlich ausländischer Kämpfer zu identifizieren.

Die britische Bürgerrechtsorganisation Statewatch protestierte gegen die Resolution und warnte vor einer weltweiten Massenüberwachung vor allem von Flugreisenden. Damit werde die Tür geöffnet für ein Instrumentarium, mit dem im großen Stil vorsorglich Profile über Flugpassagiere erstellt werden könnten. Künftig dürften etwa auch der Schiffs- oder der Zugverkehr eingeschlossen werden; EU-Staaten wie Belgien, Großbritannien, Frankreich oder die Niederlande arbeiten schon an geeigneten Systemen.

Die UN-Staaten sollen laut dem Sicherheitsrat auch Beobachtungslisten für „bekannte und verdächtige" Terroristen oder Datenbanken aufsetzen. Mit Hilfe der Technik müssten Strafverfolger, Grenzschützer, der Zoll, das Militär und Geheimdienste Reisende kontrollieren sowie Risikoeinschätzungen und Untersuchungen durchführen können. An die Mitgliedsstaaten wird appelliert, gewonnene Informationen bi- oder multilateral untereinander auszutauschen. Es soll ihnen dabei auch möglich sein, Material der Nachrichtendienste für offizielle Bedrohungsanalysen herabzustufen, also von der Geheimhaltungspflicht zweckbezogen auszunehmen. Statewatch erinnert in diesem Zusammenhang daran, dass derlei Informationen nicht immer den rechtlichen Standards entsprechen, denen Polizeibehörden folgen müssten.

In der Europäischen Union (EU) gibt es schon eine Richtlinie zum Sammeln und Auswerten von PNR, wonach neben Name, E-Mail-Adresse, Telefon-, Konten- und Kreditkartennummern auch Vielflieger-Einträge erfasst werden sollen. Der Bundestag hat im April 2017 ein Gesetz verabschiedet, wonach der Staat Flugpassagierdaten 5 Jahre lang speichern und automatisiert mit Sicherheitsdateien abgleichen kann. Die EU-Vorgaben sind aber heftig umstritten. Der Europäische Gerichtshof (EuGH) stoppte im Juli 2017 das transatlantische PNR-Abkommen mit Kanada (DANA 2017, 174 f.). Für DatenschützerInnen, BürgerrechtlerInnen, Linke, Grüne und Liberale bedeutet das auch das Aus für die EU-Richtlinie.

Der EU-Rat hat zudem im November 2017 ein geplantes biometrisches Ein- und Ausreisesystem auf den Weg gebracht. Von 2020 an sollen Fingerabdrücke und Gesichtsbilder von Angehörigen von Drittstaaten aufgenommen werden. KritikerInnen wittern auch darin einen Verstoß gegen die EU-Grundrechte. Parallel will die EU-Kommission eine virtuelle „Biometrie-Superdatenbank" mit übergreifenden Suchmöglichkeiten erstellen (Krempl, UN-Sicherheitsrat verlangt weltweit Abgleich von Fluggastdaten und Fingerabdrücken, www.heise.de 08.01.2018).

EU

Google legt Zahlen zu Link-Sperrung bei Search vor

Am 27.02.2018 teilte der Suchmaschinen-Konzern Google mit Zahlen zum Entfernen von Suchergebnissen (Google Search) in einem Bericht über die ersten drei Jahre der Umsetzung des „Rechts auf Vergessenwerden" mit. Die Anlässe waren unterschiedlich: ein Opfer sexuellen Missbrauchs, ein Mann, der beschuldigt worden war, seine Frau umgebracht zu haben, ein Forscher, der sich einer Geschlechtsumwandlung unterzogen hat und ein altes Foto von sich nicht mehr im Netz sehen wollte.

2014 hatte der Europäische Gerichtshof geurteilt, dass EU-BürgerInnen beantragen können, dass veraltete Informationen sowie verletzende Informationen über sie nicht mehr verlinkt werden, soweit dem nicht von besonderem öffentliches Interesse entgegensteht (dazu Leutheusser-Schnarrenberger, DANA 2016, 56 ff.). Ab Mai 2018 gibt es dann in der Datenschutz-Grundverordnung in Art. 17 explizit ein solches Recht.

Die Zahlen geben detailliert Auskunft über Umfang und Art der Anträge. Bis Ende 2017 stellten danach etwa 400.000 Personen oder Unternehmen aus der gesamten EU 2,37 Millionen Anträge. Die meisten Antragstellenden sind normale Menschen ohne besondere Prominenz. Seit Januar 2016 waren sie für 85% der Beanstandungen verantwortlich. Prominente stellten 4%, Politiker oder Regierungsvertreter 3% und Unternehmen 2%. Den Deutschen ist wohl besonders wichtig, vergessen zu werden: Von hier aus versuchten Antragstellende, 409.000 Links und Adressen unsichtbar zu machen. 48%, also etwa 200.000, wurden tatsächlich gesperrt.

Die Durchsetzung des Rechts auf Vergessenwerden erfolgt in starkem Maße in professioneller Form. 0,25% der Antragstellenden haben gut 20% der gesamten Links entfernen lassen. Laut Google handelt es sich um Kanzleien und Firmen, die sich um die Reputation von Klienten kümmern. Der größte Teil dieser Gruppe (17%) agiere von Deutschland aus. Am häufigsten richteten sich Anträge gegen Verlinkungen auf die sozialen Netzwerke Facebook, Google Plus, Youtube und Twitter (Deutsche ließen 200 000 Google-Links entfernen, SZ 28.02.2018, 17).

EU

PSD2-Richtlinie ermöglicht Zugriff auf Kontodaten

Seit dem 13.01.2018 gilt die sogenannte PSD2-Richtlinie (Payment Service Directive 2), mit der mehr Wettbewerb zwischen Banken und Finanzdienstleistern geschaffen und für VerbraucherInnen das Banking bequemer, billiger und sicherer gemacht werden soll. Gleichzeitig nimmt die Richtlinie die Verbraucher aber auch stärker in die Pflicht. Die Richtlinie gilt vorrangig bei Kartenzahlungen für Anbieter von Vier-Parteien-Kartensystemen, Überweisungen und Lastschriften. Sie kommt zum Zug, wenn ein Verbraucher über seine Bank eine Kreditkarte eines weiteren Anbieters bezieht. Bei einem Drei-Parteien-Kartensystem, bei dem die kartenausgebende Bank zugleich auch die Händlerbank ist, muss PSD2 im Grunde nicht angewendet werden. Eine weitere Ausnahme sind Online-Bezahldienste, die Kreditkarten- und Lastschriftzahlung in einem Wallet hinterlegen.

Mit den neuen europäischen Regeln zum Zahlungsverkehr sind einige positive Neuerungen verbunden, so Frank-Christian Pauli, Finanzexperte des Verbraucherzentrale Bundesverband (vzbv), z. B. der Wegfall von Transaktionsgebühren bei den wichtigsten Zahlungsinstrumenten bei manchen Anbietern als auch ein besserer Schutz, wenn unbefugt vom Konto oder von der Karte abgebucht wurde. Händler dürfen also künftig nicht mehr Zusatzgebühren für bestimmte Zahlungsarten verlangen. Der Verbraucher kann ohne Sorge vor Aufschlägen frei wählen, ob er etwa per Überweisung, Lastschrift oder Kreditkarte zahlt. Zu begrüßen ist zudem, dass die Haftungsgrenze für die KundInnen sinkt: Wer mit Giro- oder Kreditkarte online bezahlt, haftet für Schäden nur noch bis 50 und nicht mehr bis 150 €. Banken müssen unbefugte Buchungen schneller rückabwickeln. Hotels oder Autovermieter dürfen nur noch nach ausdrücklicher Zustimmung der KundIn einen Betrag auf deren Kartenkonto reservieren.

Neu aber ist auch, dass künftig Zahlungsdienstleister und Kontoinformationsdienste auf das Bankkonto zugreifen können, wenn die VerbraucherIn das erlaubt. Dazu Verbraucherschützer Pauli: „Unsere Bank weiß, woher wir unser Geld bekommen. Unsere Bank weiß, wie wir wann was bezahlen, ob wir unterhaltspflichtig sind, ob wir häufig in Apotheken gehen, ob wir uns häufig und wann im Ausland aufhalten und ähnliche Informationen. Und diese Informationen sind auch für die Märkte sehr interessant. Deshalb versuchen viele Anbieter, an solche Informationen zu kommen." Mit der nun erfolgenden Zulassung von Kontoinformationsdiensten können und dürfen diese künftig mithilfe der Kontozugangsdaten, die sie vom Verbraucher abfragen, auf die Kontodaten zugreifen. So erlangt der Drittdienst weitreichende Informationen.

Miriam Wohlfarth, Geschäftsführerin des Ratenzahlungsdienstleisters Ratepay sieht hierin eine Chance für Finanztechnologieunternehmen: „Theoretisch ist es jetzt bald möglich, dass Firmen entstehen, die zum Beispiel darüber informieren, dass komische Abbuchungen auf dem Konto sind, die irgendwelche Dienste rund um das Konto bringen. Und das ist etwas, was schon sehr interessant ist, weil ich glaube, das wird die Rolle der Banken sehr stark verändern."

PSD2 schreibt eine strikte Kundenauthentifizierung vor: Benutzername und Passwort reichen bei Online-Transaktionen alleine nicht mehr aus. Ein dynamisch erstellter Code oder eine TAN ist nun Pflicht und wird auch ab bestimmten Summen bei Online-Käufen abgefragt. Ab 30 Euro ist eine Sicherheitsabfrage notwendig. Auch die Anforderungen an das Sicherheitsmedium, zum Beispiel ein TAN-Generator oder eine Bank-App, sind gestiegen. Authentisierungen sind zudem mit biometrischen Daten wie verhaltensbasierter Mustererkennung per Stimme oder Gesicht möglich. PSD2 lässt mit der „Transaktion Risk Analysis" zu, dass Banken für bestimmte risikoarme Transaktionen die Grenze von 30 Euro auf bis zu 500 Euro anheben. Banken können also mit vertrauenswürdigen Onlinehändlern Vereinbarungen treffen, die diese Grenze auf 500 Euro erhöhen.

Art. 67 Abs. 2 lit. f PSD2 nimmt Bezug auf den Datenschutz: „Der Kontoinformationsdienstleister darf im Einklang mit den Datenschutzvorschriften Daten nicht für andere Zwecke als für den vom Zahlungsdienstnutzer ausdrücklich geforderten Kontoinformationsdienst verwenden, darauf zugreifen oder speichern." Zahlungsdienstleister und Drittdienste werden künftig von den Regulierungsbehörden beaufsichtigt.

Gemäß Pauli liegt ein gravierender Nachteil darin, dass VerbraucherInnen noch nicht einschränken können, welche Informationen die Dienstleister einsehen können: „Wir müssen, wenn wir so einen Dienst nutzen, quasi diesem Dienst unseren Hauptschlüssel zum Konto, unsere Zugangsdaten zum Online-Banking weitergeben. Und das finden wir problematisch, zum einen, weil man als Verbraucher dann nicht wirklich kontrollieren kann, auf welche Daten der Dienst tatsächlich zugreifen kann, wir Verbraucher müssen einfach vertrauen. Und das Zweite ist, dass natürlich auch Täter auf die Idee kommen könnten, sich als so einen Dienst darzustellen." Verbraucher müssten vorsichtig sein, wem sie ihre Zugangsdaten in fremde Hände geben: „Denn der kann über das Online-Banking den gleichen Unfug anfangen, der bisher auch schon mit den berühmt-berüchtigten Phishingmails getan wurde." Dieser Zugang zum Konto soll zwar eingeschränkt werden, doch noch fehlen die technischen Voraussetzungen dazu, bis die entsprechende Regelung in Kraft treten kann, wird es noch mindestens bis zum Sommer 2019 dauern (Scholtes, Was sich im Zahlungsverkehr ändert, www.deutschlandfunk.de 12.01.2018, Der Trend zur kostenfreien Onlinezahlung ist gesetzt, www.manager-magazin.de 18.01.2018).

EU

Parlament präzisiert Vorstellung zur Exportkontrolle von Überwachungstechnik

Mit der großen Mehrheit von 571 zu 29 Stimmen bei 29 Enthaltungen hat sich das Parlament der Europäischen Union am 17.01.2018 dafür ausgesprochen, dass die Vorschriften zur Exportkontrolle auch für Instrumente zur digitalen Überwachung gelten sollen. Hard- und Software, mit der sich etwa Mobiltelefone abhören, Computer hacken, Passwörtern umgehen oder Internetnutzer identifi-

zieren lassen, würde damit auf die Liste der Gegenstände wandern, deren Ausfuhr durch die zuständigen nationalen Behörden genehmigt werden muss. Autoritären Regimes soll es schwerer fallen, ihre BürgerInnen mit Überwachungstechnik aus der EU auszuspionieren, etwa von den Firmen FinFisher oder Trovicor.

Die EU-Kommission hatte 2016 den Entwurf für die Reform der Verordnung für Export von Gütern, die sowohl militärisch als auch zivil genutzt werden können, vorgelegt. Die Ausfuhr anderer sogenannter Dual-Use-Güter wie etwa Atomtechnik oder Navigationssysteme ist bereits reglementiert. Über den Kommissionsvorschlag hinaus sind die Abgeordneten nun dafür, einen verstärkten Datenschutz und eine Garantie für die Versammlungsfreiheit durch klare Kriterien und Definitionen zu verankern. Neue Risiken und Technik sollen zudem rascher in die Verordnung aufgenommen werden können.

Exporteure von Erzeugnissen, die noch nicht aufgeführt sind, aber zu Menschenrechtsverletzungen führen könnten, müssen nach Ansicht der VolksvertreterInnen sicherstellen, dass ihre Spähtechnik nicht in die falschen Hände gelangen kann. Für sie sollen die Sorgfaltspflichten gelten, auf die sich die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) geeinigt hat. Die Abgeordneten wollen zudem, dass Sanktionen in den Mitgliedsstaaten bei Verstößen gegen die Vorgaben harmonisiert werden. Die Kommission soll ein Handbuch veröffentlichen, in dem sie verdeutlicht, was künftig anhand der überarbeiteten Vorschriften erlaubt und verboten ist.

Verschlüsselungstechnik wollen die Parlamentarier dagegen von der Liste der Dual-Use-Verordnung streichen, da diese für den Selbstschutz von Menschenrechtsverteidigern unerlässlich sei. Prinzipiell müsste damit auch das Wassenaar-Abkommen zur Exportkontrolle überarbeitet werden, das bisher Kryptoprogramme mit umfasst. Die Bundesregierung war 2015 bereits mit einer Gesetzesverschärfung vorgeprescht, wonach Überwachungstechnik für die Telefonie und zur Vorratsdatenspeicherung genehmigungspflichtig sein soll. Auf EU-Ebene muss nun der Ministerrat seinen Standpunkt festlegen, bevor es auf die Suche nach einem Kompromiss mit dem Parlament gehen kann (Krempl, Überwachungstechnik: EU-Parlament stimmt für schärfere Exportregeln, www.heise.de 17.01.2018).

Belgien

Facebook drohen 250.000 € Strafe pro Tag

Ein belgisches Gericht hat Facebook in erster Instanz dazu verpflichtet, die Webseiten-Zugriffe von Nutzenden außerhalb des sozialen Netzwerks nicht mehr zu überwachen und die bisher gesammelten Daten zu löschen. Dies gilt für alle belgischen Internetnutzende, auch für solche, die kein Facebook-Konto haben. Bei einem Verstoß droht pro Tag eine Strafe von 250.000 Euro. Das Gericht in Brüssel begründete sein Urteil damit, dass Facebook seine KundInnen nicht ausreichend über die weitreichende Datensammlung mit Cookies und unsichtbaren Pixeln auf Webseiten von Drittanbietern informiere. Es legt nicht offen, was mit den Informationen geschieht und wie lange diese gespeichert werden.

Auch in Deutschland steht Facebook wegen Datenschutzvergehen vor Gericht. Nach einem noch nicht rechtskräftigen Urteil des Landgerichts Berlin vom 16.01.2018 verstößt Facebook gegen geltendes Verbraucherrecht, weil Voreinstellungen rechtswidrig seien und Nutzer ihren echten Namen verwenden müssen (s. u. S. 60). Das Bundeskartellamt untersucht ebenfalls seit 2016 in einem Verwaltungsverfahren mögliche Datenschutzverletzungen des sozialen Netzwerks. In einer vorläufigen Einschätzung im Dezember 2017 kam das Kartellamt zum dem Schluss, dass Facebook seine marktbeherrschende Stellung missbrauchen könnte (s. o. S. 35; Hirsch, Facebook drohen wegen Datenschutzvergehen pro Tag 250.000 Euro Strafe, www.heise.de 17.02.2018).

Dänemark

Mehr Kfz-Kennzeichen-Scanning an der Grenze

Das dänische Parlament hat sich am 22.12.2017 darauf verständigt, die Kontrollen an den Grenzübergängen nach Deutschland zu verschärfen. In Kopenhagen wurde der Haushalt verabschiedet, aus dem die verstärkten Kontrollen finanziert werden sollen. Die Pläne sehen vor, an allen Grenzübergängen automatische Nummernschild-Scanner aufzubauen. An den fünf großen Übergängen – darunter drei bei Flensburg und einer am Fährhafen in Rødby, wo die Fähren Richtung Fehmarn ablegen – sind zudem Kontrollhäuschen geplant. An den anderen Übergängen wird stichprobenartig mit Streifenwagen kontrolliert, wenn nötig aber auch mit Zivilwagen und aus der Luft. Dänemark lässt sich die verschärften Kontrollen umgerechnet 15 Millionen Euro kosten (Dänemark entscheidet: Noch schärfere Kontrollen, www.ndr.de 22.12.2017).

Österreich

Kurzzeitig Gesichtserkennung in der Apotheke

In zwei österreichischen Apotheken setzte der Pharmakonzern Bayer Austria testweise Gesichtsscanner ein, woraufhin Displays Werbung anzeigten, die zum Geschlecht und Alter der davor stehenden KundInnen passen sollten. Der Test war zunächst auf die beiden Standorte beschränkt. Ein Scanner stand als Aufsteller neben einem Medikamentenregal, ein anderer auf dem Tresen. Beide Scanner waren mit Werbedisplays ausgestattet. Außerdem befand sich noch ein drittes Display in der Apotheke. Neben den Kameralinsen war die Zeichnung eines Kopfes zu sehen, dazu der Schriftzug „Gesichtsscan". Zusätzlich informierte ein Aushang die Kunden darüber, dass sie gefilmt werden. Die Warnung vor der Kamera stand aber nicht ganz oben im Aushang. KundInnen mussten sich zunächst durch verklausulierte Sätze arbeiten, in denen unter anderem ein „digitales Point-of-Sales-Konzept" angepriesen wurde.

Einer Sprecherin von Bayer Austria zufolge wurden die Aufnahmen der Kamera nur lokal bearbeitet und weder gespeichert noch weitergereicht. Der Scanner bestimme das Geschlecht und das ungefähre Alter des Kunden.

Daraus entstehe ein Zahlenwert, ein sogenannter Hash. Die ursprüngliche Aufnahme werde sofort gelöscht. Die Geräte seien aber mit dem Internet verbunden und würden ferngewartet. Die Daten würden auch nicht weiter verknüpft werden. Nach dem Scan bekämen KundInnen auf Alter und Geschlecht angepasste Werbung zu sehen. Ältere KundInnen könnten etwa Werbung für ein Vitaminpräparat angezeigt bekommen. Ein Beispielfoto von Bayer Austria pries die Werbedisplays mit einem Mittel gegen Erkältungen an. Welches Geschlecht oder welche Altersgruppe diese Werbung ansprechen sollte, konnte die Sprecherin nicht sagen. Auch ging die Sprecherin nicht näher auf die Frage ein, welchen wirtschaftlichen Nutzen die Geräte haben. Im Fokus stehe das Testen einer Kundenansprache, hieß es.

Die deutsche Bürgerrechtsorganisation Digitalcourage bezeichnete die Gesichtserkennung in Apotheken als ungefragtes Eindringen in die Privatsphäre: „Bayer informiert zwar darüber, aber von einer Einwilligung kann nicht die Rede sein". Wer nicht überwacht werden wolle, müsse woanders einkaufen, das sei eine „Friss-oder-Stirb-Mentalität".

Ähnliche Geräte wie Bayer hatten in Deutschland bereits die Deutsche Post und die Supermarktkette Real getestet. Digitalcourage hatte deshalb im Sommer 2017 mit Verweis auf das Bundesdatenschutzgesetz Anzeige erstattet. Wenig später hatte Real den Test beendet. So ging es auch den Scannern in den Apotheken, nachdem nur kritische Berichte hierüber veröffentlicht wurden (Meineck, Sie sehen aus, als könnten Sie Vitamine brauchen, www.spiegel.de 25.11.2017).

Finnland

Test mit Führerschein-App

Die finnische Verkehrsagentur Trafi plant als erste in Europa, Führerscheine auch als Smartphone-App auszugeben. Seit Mitte Dezember 2017 testen etwa 1.000 finnische AutofahrerInnen dieses digitale Dokument. Die analoge Version sieht in Finnland fast aus wie in Deutschland: eine Plastikkarte in Kreditkartengröße, blass rosafarben, mit Foto, Name, Geburtsdatum und Angaben darüber, welche Fahrzeuge man fahren darf. Die neue Führerschein-App zeigt all diese Informationen auf dem Handy-Display, inklusive einer Art Wasserzeichen, das man sehen kann, wenn man das Gerät etwas kippt. Zur Sicherheit ist zudem der Hintergrund animiert und verändert sich dort, wo man mit dem Finger über den Bildschirm streicht. Damit sollen Fälschungen verhindert werden.

Knöllchen für Rasende kann die Behörde dank der App direkt auf deren Handy schicken. Außerdem kann man Informationen über sein Fahrzeug abfragen, etwa, wie viel Steuern es kostet. Viele FinnInnen nutzen den Führerschein, um sich auszuweisen, etwa wenn sie Alkohol kaufen oder Pakete abholen. Die Post hat erklärt, dass ihr die digitale Version dafür reicht. Trafi hat bei Autoverleihern und Autohäusern Werbung für die neue App gemacht. Ziel ist auch, das Portemonnaie mit all dem Plastik darin überflüssig zu machen. Apps zum Bezahlen gibt es in den nordischen Ländern schon viele.

Damit der digitale Führerschein vor der Polizei bei Verkehrskontrollen anerkannt wird, müssen die Finnen erst Gesetze anpassen. Der Pilotgruppe um Simo Karppinen, der bei Trafi die Abteilung für Führerscheine leitet, wurde daher von der Polizei empfohlen, der physische Führerschein solle noch mitgeführt werden. Es werde wohl einige Jahre dauern, bis die App die Plastikkarte völlig ersetze.

Um das Problem auch auf europäischer Ebene zu lösen, gibt es eine Arbeitsgruppe, angesiedelt im Verband europäischer Kfz-Zulassungsstellen. Simo Karppinen sitzt in dieser Arbeitsgruppe. Er weiß daher, dass andere Länder, z. B. Großbritannien und die Niederlande, ebenfalls schon ziemlich weit sein sollen mit ihren Führerschein-Apps. Die finnische App „Autoilija" soll im Sommer 2018 für alle FinnInnen verfügbar sein, die ein Smartphone und eine Fahrerlaubnis haben.

Finnland ist App-Land. Nachdem Nokia mit seiner Handysparte den Anschluss ans iPhone verpasst hatte, entwickelte sich in dem Land eine Gründerszene um die Frage, was man mit einem Handy sonst noch anstellen kann. Die Spiele-Apps Angry Birds und Clash of Clans stammen aus diesem Land. Inzwischen gibt es Apps für fast alle Lebenslagen. Ganze Städte sollen smart werden. Dort schalten die kleinen Handy-Programme dann Kaffeemaschinen aus der Ferne aus und überwachen den Energieverbrauch der Sauna. Man kann mit ihnen Taxis rufen, Autos ausleihen und Reisen planen (Bigalke, Knöllchen aufs Handy, SZ 13.02.2018, 1).

Lettland

DDOS-Attacke auf elektronisches Gesundheitssystem

Unbekannte Hacker haben offenbar mit einer DDoS-Attacke das Angebot des elektronischen Gesundheitssystems in Lettland lahmgelegt. Der zuständige Staatssekretär des Gesundheitsministeriums Aivars Lapins erklärte am 16.01.2018, es habe sich um einen gezielten Angriff durch bisher unbekannte Hacker gehandelt. Daten seien, so das Ministerium und die für Internetsicherheit zuständige Behörde, nicht gefährdet gewesen. Die Seite wurde nach Angaben des Gesundheitsministeriums in Riga mit einer Vielzahl externer Anfragen lahmgelegt. Diese DDoS-Attacke sei von Computersystemen aus mehr als 20 Ländern in und außerhalb der EU durchgeführt worden. Der externe Zugriff auf das digitale Gesundheitsinformationssystem sei unmittelbar nach der Attacke vorübergehend gesperrt worden. Zuvor hatte die Vorsitzende des Ausschusses für Arbeit und Soziales im lettischen Parlament von Störungen des Systems durch Hacker berichtet. Das zentrale Gesundheitsinformationssystem wurde 2016 in Betrieb genommen. Darüber können etwa papierlose Rezepte ausgestellt werden. Trotz Widerstands von ÄrztInnen müssen sich seit Jahresbeginn 2018 alle Gesundheitseinrichtungen in Lettland verbindlich dem System anschließen. Dieses wies wiederholt technische Probleme auf (Internet-Attacke gegen Lettlands elektronisches Gesundheitssystem, www.heise.de 17.01.2018).

Großbritannien

Sechsstelliges Schmerzensgeld für Grant wegen Abhörangriffen

Wegen eines Abhörangriffs auf sein Handy soll der 57 Jahre alte britische Filmstar Hugh Grant eine sechsstellige Summe erhalten. Darauf einigten sich der Schauspieler und die Verlagsgruppe Mirror Group vor Gericht. Journalisten dieser Publikationsorgane hatten ihn und weitere Prominente zwischen den Jahren 1998 und 2010 ausspioniert, indem sie sich Zugang zu deren persönliche Accounts beschafft hatten. Zur Mirror Group gehören die britischen Zeitungen „Daily Mirror", „Sunday Mirror" und „Sunday People". Neben Grant waren u. a. auch die Mobiltelefone von Schauspielerin Michelle Collins und Ex-Fußballer Kevin Keegan betroffen. Nach der gerichtlichen Anhörung erklärte Grant: „Meine Anwältin und ich wollten diesen Rechtsstreit weiterführen, weil ich unbedingt die Wahrheit über das Wesen der hochgradigen Verschleierungen der Mirror Group herausfinden wollte."

Hugh Grant erklärte, er werde das Geld der Kampagne „Hacked Off" spenden. Die Organisation kümmert sich seit 2011 um Opfer von Abhör-Attacken durch Journalisten. Die ehemalige Polizistin und TV-Moderatorin Jacqui Hames erzielte unterdessen eine Einigung mit dem Zeitungsverlag News Group Newspapers. Die inzwischen eingestellte Boulevardzeitung „News of the World" stand 2011 im Zentrum eines Abhörskandals durch Journalisten in Großbritannien. Hugh Grant hatte sich bereits 2012 mit dem Verlag auf einen Vergleich geeinigt (Hugh Grant erstreitet sechsstellige Summe vor Gericht, www.rp-online.de 05.02.2018).

USA

Nebula plant Gendaten-Selbstvermarktung

Das US-amerikanische Start-up Nebula Genomics aus Boston plant, das Erbgut privater KundInnen für 1000 Dollar zu entschlüsseln und ihnen zudem anzubieten, die durch ein Blockchain-Verfahren gesicherten DNA-Sequenzen an Pharmaunternehmen zu vermieten, damit diese damit Forschung betreiben können. Transaktionen sollen mit einer eigens aufgelegten Kryptowährung „Nebula tokens" abgewickelt werden. Für die Datenpächter, die Transparenz über ihre Identität herstellen müssen, sollen die Betroffenen anonym bleiben. Kamal Obbad, einer der Gründer erklärte: „Wir versuchen, normale Menschen zu überzeugen, dass sie nicht nur ihre genetische Daten zu Geld machen können." Hinter der Firma steht auch der Harvard-Genetiker George Church, der daran arbeitet, die Erbgutanalyse zu „demokratisieren", um mehr Daten für die Forschung zu generieren. Konkurrenten in die USA wie 23andMe oder Ancestry.com verwerten die Daten ihrer KundInnen selbst. Das Nebula-Genomics-Netzwerk sol dagegen „ohne Mittelsmann" funktionieren. Church und sein Team rechnen mit einem „Milliardenmarkt". Die personalisierte Genomsequenzierung werde die Diagnose und die Krankheitsprävention verbessern, personalisierte Therapien ermöglichen und die Entwicklung neuer Medikamente vorantreiben. Andere Start-ups wie EncrypGen, Luna DNA und Zenome entwickeln nach eigenen Angaben ebenfalls Plattformen, über die Betroffene ihre Gen-Informationen online verkaufen können, doch bieten sie selbst keine Genom-Sequenzierungen an (Mit eigenen Genen Geld verdienen, Der Spiegel 8/2018, 107; Mattke, Mit den eigenen Gen-Daten per Blockchain handeln, www.heise.de 13.02.2018).

Türkei

Terrorismusverdacht wegen installierter Kommunikations-App

Die türkische Regierung hat nach dem gescheiterten Putsch im Sommer 2016 per Notstandsdekret mehr als 140.000 Menschen aus dem Staatsdienst entlassen oder suspendiert. Den meisten wird vorgeworfen, der Bewegung des in den USA lebenden Predigers Fethullah Gülen anzugehören. Als Beleg diente den Behörden die Kommunikations-App „ByLock" auf den Handys der Verdächtigen. Im Januar 2018 machte die Regierung – wieder per Dekret – die Entlassung von 1.800 gefeuerten BeamtInnen rückgängig, darunter 460 aus dem Polizeidienst, weil die „ByLock"-App ohne deren Wissen installiert worden sein soll.

Die Regierung hält die Gülen-Bewegung für die treibende Kraft hinter dem Putschversuch vom Juli 2016. Seitdem versucht sie systematisch Gülen-AnhängerInnen aus dem Staatsapparat zu entfernen. Nach Überzeugung der Regierung ist ByLock ein speziell von der und für die Gülen-Bewegung entwickeltes Werkzeug zur verschlüsselten Kommunikation. Wer die App heruntergeladen hatte, galt als Verschwörer; Staatsanwälte und Richter schlossen sich dieser Auffassung an. Zigtausende Menschen verloren ihren Job, mehr als 50.000 kamen – zumindest zeitweise – in Haft. Auch dem Amnesty-Chef Taner Kılıç wurde die App zum Verhängnis; er sitzt in Haft. Der prominente Journalist Kadri Gürsel kam für fast ein Jahr ins Gefängnis, weil ByLock-Nutzer versucht hatten, ihn zu kontaktieren. Dabei hatte Gürsel die Gülen-Bewegung immer wieder kritisiert – der Vorwurf, er sympathisiere mit ihr, war abwegig. Auch wegen solcher Absurditäten kritisieren türkische Oppositionelle und ausländische Beobachter die Praxis scharf, ByLock-Nutzende pauschal zu Terrorverdächtigen zu machen.

Für einen Teil der Betroffenen gibt es nun die Chance auf Rehabilitierung: Seit kurzem verweisen Regierung und Justiz auf ein Programm namens „Mor Beyin", das auf den Geräten von mehr als 11.000 Menschen ohne deren Wissen ByLock installiert habe. Mit Mor Beyin habe die Gülen-Bewegung von ihren tatsächlichen Anhängern ablenken wollen, erklärte Ende Dezember 2018 der Oberstaatsanwalt in Ankara. Erwartet wird, dass bald weitere Staatsbedienstete in ihre Jobs zurückkehren dürfen. Die 1.800 gerade rehabilitierten BeamtInnen mussten dann binnen zehn Tagen auf ihre Posten zurückkehren; ihnen steht der entgangene Lohn zu, aber keine Entschädigung (Seeling, Verhängnisvolle App, SZ 13./14.01.2018, S. 8).

Russland

Spionieren U-Boote Nordatlantik-Überseekabel aus?

Die Nato ist über zunehmende Aktivitäten russischer U-Boote in der Nähe wichtiger Datenkabel im Nordatlantik alarmiert. Gemäß hochrangigen Militärvertretern in Brüssel haben die Operationen ein Ausmaß erreicht, wie es der Westen seit Ende des Kalten Krieges nicht mehr erlebt hat. Die Kabel stellen den Internetverkehr und andere Kommunikationsverbindungen nach Europa und Nordamerika sicher. Über diese Kanäle würden auch täglich Handelsgeschäfte im Umfang von Billionen Dollar abgewickelt. Wenn es gelänge, diese Verbindungen zu kappen, hätte das immense Folgen für die globale Wirtschaft. Würden die Kabel angezapft, könnten sie Moskau wertvolle Einblicke in den internationalen Internetverkehr geben.

US-Admiral Andrew Lennon, der Kommandeur der U-Boot-Streitmacht des westlichen Bündnisses, wird zitiert: „Russland zeigt klar ein Interesse an der Unterwasser-Infrastruktur der Nato und der Nato-Länder". Die Nato plane deshalb zur Sicherung des Nordatlantiks die Wiedereröffnung eines nach dem Kalten Krieg geschlossenen Kommandopostens. Auch arbeiteten Nato-Verbündete daran, ihre Anti-U-Boot-Kampfkapazitäten zu verbessern. Zudem hätten die Aktivitäten den Westen zur Wiederbelebung ihrer Fähigkeiten zur U-Boot-Jagd gezwungen. Das habe man zwar auch nach dem Kalten Krieg immer wieder geübt, aber in den vergangenen Monaten sei es notwendig geworden, das Aufspüren tatsächlich zu praktizieren (Russische U-Boote haben Datenkabel im Nordatlantik im Visier, www.heise.de 23.12.2017).

Russland

Facebook darf Daten nicht im Ausland speichern

Der oberste „Datenschützer" Russlands, der Leiter der Aufsichtsbehörde für Medien, Telekommunikation und Datenschutz, Alexander Scharow, forderte am 26.09.2017 von Facebook, die Nutzerdaten russischer BürgerInnen künftig nur noch lokal zu speichern. Andernfalls werde das soziale Netzwerk gesperrt. Das soziale Netzwerk würde gegen das russisches Recht verstoßen, wenn es ab 2018 Nutzerdaten von RussInnen nicht auf heimischen Servern speichere. Sollte sich Facebook weigern, müsse das Unternehmen seine Arbeit in Russland einstellen. Das Gesetz über die Speicherung personenbezogener Daten gilt in Russland seit 2015. Seit 2016 ist das Karriere-Netzwerk LinkedIn dort nicht mehr zugänglich. Das Unternehmen hatte gegen die drohende Sperre geklagt, war aber vor Gericht zweimal gescheitert. Facebook hat nach der Aufforderung nun bis 2018 Zeit, der Forderung zu entsprechen. Die Moskauer Führung versucht seit Jahren, das Internet in Russland stärker zu kontrollieren. Im Sommer 2017 hatte das russische Parlament, die Duma, zudem ein Gesetz beschlossen, das die Nutzung von Anonymisierungs-Software und sogenannter Virtueller Privater Netzwerke (VPN) im Internet einschränkt (Bube, Russische Aufsichtsbehörde droht Facebook mit Sperre, http://www.crn.de/software-services/artikel-114927.html, 26.09.2017).

USA – weltweit

Supreme Court entscheidet über Datenzugriff im Drittausland

Im Juni 2018 urteilt voraussichtlich der US Supreme Court in Washington, D.C., über den Zugriff von US-Ermittlern auf Daten von Internet-Unternehmen, also über den Zugriff auf E-Mails, Steuererklärungen, Dokumente, Fotos, Kontakte, abgerufene Webseiten und damit über fast sämtliche in Europa generierten Daten, die in einer Cloud gespeichert sind. Für den US-Daten-Zugriff genügt es, wenn das Unternehmen, das die Daten verwaltet, auch in den USA tätig ist. Die Vereinten Nationen (UNO), die EU-Kommission, die Regierungen Irlands und Großbritanniens und sogar konservative ehemalige US-Regierungsbeamte haben sich mit sogenannten Amicus-Briefen in dem Verfahren eingebracht. Auch die deutschen Industrieverbände BDI und DIHK bringen sich ein. In den USA sind in solchen Verfahren Unbeteiligten Stellungnahmen möglich.

Das US-Justizministerium ermittelte in einem Fall von Drogenkriminalität und verlangte 2013 von Microsoft Zugriff auf das E-Mail-Konto eines Verdächtigen. Ein New Yorker Bezirksrichter hatte einen entsprechenden Durchsuchungsbefehl ausgestellt und sich dabei auf ein Gesetz von 1986 berufen. Der Server mit den Daten stand aber in Irland. Microsoft erklärte, hierfür sei ein New Yorker Durchsuchungsbeschluss nicht gültig. Den ersten Prozess verlor Microsoft, in der zweiten Instanz siegte das Unternehmen. Nun entscheidet der Supreme Court. Wie dessen Urteil ausfallen wird, gilt als offen. Die US-Regierung argumentierte für den Datenzugriff mit dem Hinweis auf die abzuwehrende Terrorismusgefahr.

In den Stellungnahmen gegenüber dem Gericht warnen alle bis auf die Briten eindringlich davor, US-Ermittlern den Zugriff auf Daten im Ausland zu erlauben. Die EU-Kommission drängt darauf, dass die USA sich an internationales Recht und Gepflogenheiten halten. Wer Daten wolle, könne und müsse sie über bereits bestehende internationale Abkommen anfordern. Irland betont in seinem Schreiben, dass es bereit sei, den USA die Daten auf diesem Wege zur Verfügung zu stellen. Das Vorgehen des US-Justizministeriums aber wertet die irische Regierung als Angriff auf ihre Souveränität. Die Argumentation, Dublin müsse seine souveränen Rechte erst vor einem US-Gericht erklären, damit sie wirksam seien, lehne man strikt ab. Sollte Irland nicht in einem US-Prozess intervenieren, heiße das keineswegs, dass es eine Verletzung seiner Souveränität hinnehme.

Erstaunlich ist, dass kritische Stellungnahmen auch von ehemaligen US-Justiz-, Sicherheits- und Geheimdienstbeamten kommen, darunter prominente Konservative wie der frühere US-Heimatschutzminister Michael Chertoff. Sollte das Justizministerium vor dem Supreme Court siegen, gäbe es ein juristisches Chaos, so Chertoff, das die grenzüberschreitende Verbrechensbekämpfung und Geheimdienstzusammenarbeit gefährde. Es drohe eine „Balkanisierung des Internets", wenn Staaten gezwungen würden, wichtige Daten nur

noch innerhalb ihrer eigenen Grenzen zu speichern, um sie vor Zugriffen aus dem Ausland zu schützen. Auch der Grünen-Europaabgeordnete Jan-Philipp Albrecht meinte: „Das würde das Internet in seiner heutigen Form zerstören". Joseph Cannataci, Uno-Sonderberichterstatter für das Recht auf Privatsphäre, wies darauf hin, dass die Erlaubnis des Datenzugriffs dazu führen würde, dass nicht nur US-Ermittler außerhalb ihrer Landesgrenzen aktiv würden. Sollte der Supreme Court es einem Land gestatten, einseitig Daten aus anderen Staaten abzugreifen, hätte das gravierende Folgen für die Rechte der Internetnutzer weltweit – insbesondere wenn „Staaten ohne Respekt vor Rechten" sich diese Praxis zu eigen machten. Dies sieht der Grünen-Politiker Albrecht genauso: „Die Chinesen würden von Unternehmen, die in China sitzen oder dort tätig sind, dann auch Daten verlangen – auch von amerikanischen". Vorstellbar wäre, dass türkische Ermittler bei der Google-Filiale in Istanbul vorstellig werden und die E-Mails in Deutschland lebender angeblicher Staatsfeinde verlangen, oder dass russische Strafverfolger bei Microsoft in Moskau ähnliches tun.

Wirtschaftsverbände befürchten „weitreichende Konsequenzen für Millionen von Firmen" im Fall eines gerichtlichen Siegs des US-Justizministeriums. Gemäß dem Bundesverband der Deutschen Industrie (BDI) und dem Deutschen Industrie- und Handelskammertag (DIHK) sowie den entsprechenden irischen, polnischen und französischen Verbänden würde ein solches Urteil „praktisch jeden grenzüberschreitenden Datenverkehr betreffen". Unternehmen stünden vor einem Dilemma: Sie müssten entweder gegen das Recht an ihren Standorten verstoßen oder US-Behörden missachten.

Albrecht wies darauf hin, dass die EU-Behörden ab Mai 2018 die Datenschutz-Grundverordnung durchsetzen müssen: „Der Europäische Gerichtshof kennt keine Gnade, was die Umsetzung von EU-Recht gerade in diesem Bereich betrifft. Firmen wie Microsoft bliebe dann wohl nur noch die Abspaltung jener Unternehmensteile, die in der EU Dienste anbieten, oder der Rückzug aus Europa.

Zwar hat sich die EU-Kommission „im Namen der Europäischen Union" an den Supreme Court gewandt, doch hinderte dies das Noch-EU-Mitglied Großbritannien nicht daran, einen eigenen Brief nach Washington zu schicken und darin der Linie der EU zu widersprechen. Es macht sich die Argumentation der US-Regierung vollständig zu eigen. In welchem Land Daten gespeichert sind, „sollte nicht darüber entscheiden, ob eine Nation Zugang zu diesen Kommunikationsdaten bekommt". Der Versuch des US-Ministeriums, Daten einer in den USA tätigen Firma zu erhalten, sei auch kein Fall von „extraterritorialer Rechtsprechung". Der Brief der britischen Regierung verrät ein pikantes Detail: London und Washington arbeiten demnach an bilateralen Abkommen, „um den gegenseitigen Zugang zu Kommunikationsdaten zu erleichtern". Ein Sieg Microsofts wäre dem hinderlich.

Ein Mitarbeiter der EU-Kommission kommentierte: „Die Briten suchen dermaßen verzweifelt nach Freunden, dass sie sich aufführen wie die Lobbyisten Washingtons." Statt ihren Verpflichtungen gegenüber der EU nachzukommen, arbeiteten sie für die Zeit nach dem Brexit. Über den Deal mit den USA wollten sich die Briten auch in Zukunft Zugang zur Kommunikation der EU-BürgerInnen sichern. Es wäre insofern natürlich praktisch, wenn US-Ermittler auf Daten von EuropäerInnen zugreifen könnten. Doch auch die EU steckt in einer Zwickmühle: Ihre Behörden erhalten ebenfalls gern Daten aus den Beständen von Google, Microsoft und anderen großen Anbietern von Cloud-Diensten, die alle ihren Sitz in den USA haben. Die niederländische Liberale Sophia in 't Veld hält aber nichts von dieser Erwägung: „Wir sind größer als die USA, doch wir verhalten uns wie politische Zwerge. Wie sollen EU-Bürger der EU vertrauen, wenn wir nicht einmal unsere eigenen Gesetze verteidigen?" Die EU habe die Tendenz, Rechte von US-Bürgern über die von Europäern zu stellen (Becker, US-Gericht entscheidet über unsere Privatsphäre, www.spiegel.de 03.01.2018).

USA

US-Militär scannt weltweit soziale Netzwerke

Bei einem Routine-Scan fielen dem IT-Security-Experten Chris Vickery riesige Daten-Container in die Hände, die das US-Militär zur Überwachung und Manipulation sozialer Netzwerke in der Amazon-Cloud gesammelt hat. Er hatte Amazons Cloud-Speicherdienst S3 nach offenen Türen abgeklopft. Unter den Namen „Centcom-Backup", „Centcom-Archive" und „Pacom-Archive" fand er drei riesige Datencontainer mit Überwachungsdaten aus sozialen Netzwerken rund über den Globus verteilt. Der Name „Centcom" steht für die militärische Leitung der US-Streitkräfte Cental Command. „Pacom" steht für Pacific Command, also den Teil der Streitkräfte, der sich um China, Asien und Australien kümmert.

Die Datencontainer sollen dutzende Terabyte an Rohdaten aus Überwachungen sozialer Netzwerke enthalten. Vickery lud eine Probe von 400 GByte herunter mit 1,8 Milliarden Social-Media-Beiträgen aus den vergangenen acht Jahren. Die Beträge stammten gemäß seiner Analyse hauptsächlich aus Asien und den USA. Anhand der Datenstruktur und Verschlagwortung kam Vickery zu dem Schluss, dass die Rohdaten für das Outpost-Programm der US-Regierung zur Terror-Abwehr genutzt würden. Es sammle nicht nur Daten, sondern könne auch Kampagnen zur Beeinflussung starten – ähnlich wie sie die US-Regierung derzeit Russland vorwirft. So fand er Konfigurations-Dateien für Apache Lucene und die Open-Source-Engine Elasticsearch.

Andere Hinweise zeigten auf „Coral", womit das Data-Mining-Programm Coral Reef gemeint sein könnte. Mit Coral Reef sollen Analysten sehr schnell große Datenbestände durchforsten, um Verbindungen und Kontaktnetzwerke aufzustöbern. Vickery informierte das US-Militär über seinen Fund. Der Zugriff auf die Daten war ihm aufgrund einer Fehlkonfiguration der S3-Server des US-Militärs möglich. Diese bedankten sich für seine Hilfe und konfigurierten die S3-Server entsprechend um.

Vickery zeigte sich erstaunt, wie fahrlässig das US-Militär mit seiner Datensicherheit umgeht. Jeder – egal ob er den USA freundlich oder feindlich gesonnen ist – hätte freien Zugriff auf die hochsensiblen Daten gehabt und könne sie gegen die überwachten Menschen einsetzen (Gieselmann, Terabyte-große Datencontainer entdeckt: US-Militär

überwacht Soziale Netzwerke weltweit, www.heise.de 19.11.2017).

USA

Devumi verhökert per Identitätsdiebstahl gekaperte Schein-Aufmerksamkeit

Gemäß einem Bericht der New York Times von Ende Januar 2018 betreibt das US-amerikanischen Unternehmen Devumi in groß angelegtem Umfang „Identitätsdiebstahl", um seinen mehr als 200.000 KundInnen Heerscharen von „Followern, Nutzern und Likes" zu vermitteln. Mit einem Massenaufgebot von geschätzten 3 bis 5 Mio. komplett automatisierten und kompromittierten Internet-Accounts von realen Personen, die immer wieder an neue Devumi-Kunden verhökert werden, wurden diese gemäß dem Bericht bereits mehr als 200 Mio. mal als falsche Claqueure im Dienst der Devumi-Klienten zum Einsatz gebracht.

Devumi bietet käufliche Aufmerksamkeit im Internet für Stars, Sternchen des Showbiz, AthletInnen, PolitikerInnen, aber auch für ganz normale Menschen, die es in die Sphäre digitaler Beachtung drängt. Fernsehgrößen, SportlerInnen, Comedians, TED-SprecherInnen, Geistliche und Models kaufen sich bei dem Unternehmen Armeen von Schattenbegeisterten bzw. die Illusion von massenhaft bezeugter Aufmerksamkeit gegen viel Geld ein. Sogar ein Mitglied des Vorstands der Firma Twitter hat sich so mit vielen Twitter-Followern eingedeckt.

Der Beleg großer Aufmerksamkeit attestiert nicht nur großen Erfolg und eine breite soziale Akzeptanz, sie definiert auch Interesse. Und da schaut man eben hin, weil alle hinschauen. So kommt es, dass Popularität neue und oft sogar noch größere Popularität erzeugt. Diese Form der Selbsterfüllung gilt verstärkt für die Stars der sozialen Medien, die sog. Influenzer, weil sie in der digitalen Aufmerksamkeitsökonomie mit massenunterfütterter Präsenz Einfluss auf das Kaufverhalten von Gesellschaften nehmen. Und darum macht eine große Followerzahl auch das, wofür die Influenzer stehen und werben, wiederum relevant und modisch hipp. Viele Menschen, viel Aufmerksamkeit, viel Geld, so die banale Faustformel, oder gemäß dem Jargon der sozialen Medien: „Scheiße schmeckt! So viele Fliegen können sich ja nicht irren."

Devumi wirbt mit: „Dein Erfolg in den sozialen Medien, wir machen ihn möglich. Du kommst rasend schnell an Follower, Nutzer, die dich wahrnehmen, mögen & noch viel mehr" dank „unserer Kraftmischung an Marketing-Taktiken". Die realen Namen, Profil-Fotos, Adressen und Daten von mindestens 55.000 lebenden Personen wurden geplündert, u. a. Internetpräsenzen von Jugendlichen. Der Bericht schildert den Fall eines Mädchens aus Minnesota, dessen Daten zum Beifall für kanadische Immobilienmakler wie für obskure Kryptowährungen, für eine Radiostation in Ghana, zur Weiterverbreitung von Meinungen auf Arabisch und Indonesisch (Sprachen, die der Teenager gar nicht beherrscht) und natürlich (und wie fast immer) für Porno-Seiten eingesetzt wurden. Reale Menschen wurden wie Falschgeld in Umlauf gebracht.

Die sozialen Medien wie Facebook und Twitter, auf denen dieser Betrug stattfindet, verweisen auf ihre AGBs, die so etwas verbieten, viel mehr aber bisher nicht. Denn der Marktwert auch dieser Unternehmen bemisst sich nach der Zahl ihrer Nutzenden und deren Aktivitäten dort, egal ob echt oder nicht. Der Geschäftsführer der „Follower-Fabrik" Devumi wies alle Vorwürfe weit von sich. Die New Yorker Generalstaatsanwaltschaft hat dennoch mitgeteilt, dass sie Ermittlungen wegen Identitätsdiebstahl aufnehmen will (Graf, Falschgeld Mensch, SZ 30.01.2018, 13).

USA

Weinstein ließ wohl gegen Übergriffsopfer spionieren

Ronan Farrow, der 29-jährige Sohn von Regisseur Woody Allen und Schauspielerin Mia Farrow, hatte schon Anfang Oktober 2017 mit einem Beitrag im „New Yorker" den Skandal um die sexuellen Übergriffe des Hollywood-Produzenten Harvey Weinstein eskaliert, als er berichtete, dass drei Frauen, unter ihnen die italienische Schauspielerin Asia Argento und die angehende Darstellerin Lucia Evans von Weinstein angeblich vergewaltigt wurden. Einen Monat später legte er mit einer umfassenden Recherche in der gleichen Zeitschrift nach und legte ein umfassendes Spitzel- und Vertuschungssystem des Produzenten offen.

Weinstein hat danach private Sicherheitsfirmen angeheuert, um Informationen über die Frauen zu sammeln, die ihm sexuelle Belästigung und Missbrauch vorwarfen. Der Filmproduzent habe im Herbst 2016 mehrere Firmen eingeschaltet – PSOPS, Kroll und Black Cube. Black Cube schreibt von sich selbst als „ausgewählte Gruppe von Veteranen der israelischen Geheimdienste". Unter anderem sollen dort ehemalige Agenten des Mossad, also des israelischen Auslandsgeheimdienstes, als Privatdetektive tätig sein. Die Unternehmen wurden gemäß den Unterlagen damit beauftragt, sowohl potenzielle Opfer zum Schweigen zu bringen, als auch die Veröffentlichung von Artikeln über Weinstein zu verhindern. Explizit werden der „New Yorker" sowie die „New York Times" genannt. In zwei Fällen sollen auch Journalisten ins Visier geraten sein. Mit dieser „Armee von Spionen" habe die Veröffentlichung der Anschuldigungen gegen den 65-jährigen Oscar-Preisträger verhindert werden sollen. Farrow kommentierte seine Recherche und zog eine Parallele zu seiner Arbeit in Afghanistan: „Verrückteste Geschichte, über die ich je berichtet habe, und eine seltene Erfahrung, die mich um meine Sicherheit fürchten ließ."

Farrow beruft sich in dem Bericht auf Dokumente und die Aussagen von sieben beteiligten Personen. Ein Vertrag soll von Weinsteins Anwalt David Boies von der Kanzlei Boies, Schiller und Flexer, der einst auch Ex-US-Präsidentschaftskandidat Al Gore vertreten hatte, unterzeichnet worden sein. Für einen über die Anwaltskanzlei organisierten Spionageauftrag hat Black Cube eine Rechnung über 600.000 Dollar gestellt. Offenbar war auch ein finanzieller Bonus vereinbart, der fällig geworden wäre, wenn die belastenden Artikel nicht erschienen wären. Pikant ist, dass die Kanzlei gleichzeitig auch für die New York Times in anderer Angelegenheit tätig war. Die Zeitung ver-

öffentlicht am 07.11.2017 ein empörtes Statement, warf Boies Vertrauensbruch vor und kündigte mögliche rechtliche Schritte an.

Zwei Mitarbeiter von Black Cube sollen sich unter falschem Namen mit der Schauspielerin Rose McGowan getroffen haben. Die 44-Jährige zählte mit zu den ersten, die Weinstein der Vergewaltigung beschuldigten. Zuvor habe sich eine Privatermittlerin im Auftrag von Black Cube als Frauenrechtsanwältin ausgegeben und mindestens vier Treffen mit McGowan verdeckt mitgeschnitten. Farrow schlüsselt in dem Stück auf, wie die Ex-Agentin um das Vertrauen der Schauspielerin warb. Sie aß mit ihr Eis am Strand, verschickte E-Mails mit der Grußformel „Hallo Liebe" und bewunderte vermeintlichen McGowans Mut, die Übergriffe anzuprangern. McGowan beschuldigt Weinstein, sie 1997 vergewaltigt zu haben. Diese Vorgänge hat sie in einem Buch mit dem Titel „Brave" (tapfer) aufgeschrieben, das Anfang 2018 erscheint.

Dieselbe private Ermittlerin soll sich dem Bericht zufolge auch zweimal mit einem Journalisten getroffen und vorgegeben haben, selbst etwas gegen Weinstein in der Hand zu haben. So habe sie offensichtlich in Erfahrung bringen wollen, welche Frauen mit der Presse reden. Der Journalist wurde allerdings misstrauisch, er beschrieb das Auftreten des angeblichen Opfers, das sich von einer britischen Handy-Nummer bei ihm gemeldet habe, als „Seifenopern-Schauspielerei". Den Akzent der Frau habe er zunächst für deutsch gehalten. Die weiteren von Weinstein engagierten Firmen sollten offenbar Fotos sammeln und psychologische Profile über die „persönliche und sexuelle Vergangenheit" der Weinstein-Opfer zusammenstellen, um so belastendes Material in die Hände zu bekommen. Weinstein soll den Fortschritt der Untersuchungen persönlich überwacht haben.

Weinsteins Sprecherin Sallie Hofmeister erklärte dazu: „Es ist eine Fiktion, es so hinzustellen, als seien irgendwelche Personen zu irgendeiner Zeit ins Visier genommen oder unterdrückt worden." Weinstein streitet die Vergewaltigungen ab. Sein Anwalt Boies bestätigte aber, die Verträge abgeschlossen und dafür gezahlt zu haben. Er sprach von einem Fehler: „Zu dieser Zeit erschien es als vernünftige Regelung für einen Kunden, aber es war nicht durchdacht, und das war mein Fehler." Mittlerweile werfen mehr als 70 Frauen dem Hollywoodmogul sexuelle Belästigungen bis hin zur Vergewaltigung vor. Polizeibehörden in Los Angeles, Beverly Hills, New York und London ermitteln gegen ihn. Der Fall hat eine weltweite Debatte über Belästigung und sexualisierte Gewalt unter dem Hashtag „meetoo" ausgelöst (Harvey Weinstein hat offenbar Ex-Mossad-Agenten auf Opfer angesetzt, www.spiegel.de 07.11.2017; Steinitz, Ausspioniert, SZ 08.11.2017, 13).

USA

Uber bestätigt großes Hacking-Leak

Dara Khosrowshahi, seit August 2017 Vorstandsvorsitzender des Fahrdienstes Uber, entschuldigte sich Ende November 2017 erneut, diesmal für die Vertuschung eines massiven Diebstahls von Kundendaten. Im Oktober 2016 wurden Uber zufolge persönliche Informationen von 57 Mio. Kundenkonten gestohlen. Um die Hacker zum Schweigen zu bringen, zahlte das Unternehmen 100.000 US-Dollar. Khosrowshahi, der nach einigen Uber-Skandalen das Unternehmen übernommen hatte, entschuldigte sich: „Nichts davon hätte passieren dürfen und ich werde dies nicht entschuldigen." Bei dem Diebstahl wurden Namen, E-Mail-Adressen und Mobiltelefonnummern von KundInnen aus aller Welt von den Hackern kopiert. Auch die Namen und Lizenznummern von rund 600.000 Uber-FahrerInnen in den USA seien betroffen. Inwieweit Daten deutscher KundInnen in falsche Hände gelangten, ist unklar.

Laut Khosrowshahi gelangten die beiden Hacker über die Softwareentwickler-Plattform Github an Ubers Anmeldeinformationen über einen Cloud-Anbieter, wo sie die Kundendaten herunterladen konnten. Eine Github-Sprecherin meinte, der Angriff sei keine Folge von Sicherheitslücken. Uber entließ den Chef-Sicherheitsbeauftragten Joe Sullivan und einen seiner Stellvertreter.

Uber stand immer wieder wegen seiner aggressiven Expansionspolitik in der Kritik. Der Vorgänger von Khosrowshahi, der Gründer Travis Kalanick, muss sich in mehreren Straf- und Zivilverfahren wegen sexueller Belästigung und Fehlverhalten im Unternehmen verantworten. Kalanick, der weiterhin einen Verwaltungsratsposten innehat, soll gemäß Insidern bereits einen Monat nach dem Datendiebstahl in Kenntnis gesetzt worden sein.

Khosrowshahi betonte nun, Uber werde aus den Fehlern lernen. Die Sicherheitsabteilung werde neu aufgebaut und die Cyber-Firma Fire Eye schaue sich die Sicherheitslücke genauer an. Die Behörden seien informiert worden. Der Generalstaatsanwalt von New York habe ein Verfahren eröffnet. Zudem kündigten Behörden in Australien und auf den Philippinen an, den Fall zu prüfen. Bei Uber ist es nicht das erste Mal, dass es zu einem Datenklau kam. Kriminelle waren an Informationen von Fahrern gelangt und 2014 gaben Beschäftigte zu, ein Softwareprogramm genutzt zu haben, um Passagiere zu verfolgen (Ubers Entschuldiger vom Dienst, SZ 23.11.2017, 16).

Indien

Elterliche Videokontrolle des Schulunterrichts

Die Regierung im indischen Delhi will Eltern Zugriff auf vorgesehene Videoüberwachungsbilder der Klassenzimmer in öffentlichen Schulen gestatten. Mit Hilfe einer dafür noch in der Entwicklung befindlichen App können sie dann in Echtzeit Schulklassen beobachten. Jedes Elternteil soll eine eindeutige Login-ID erhalten. Ein Vertreter des regionalen Bildungsministeriums sagte, die App werde es Eltern ermöglichen, Live-Übertragungen aus dem Klassenzimmer der eigenen Kinder einzusehen: „Eltern müssen die Nummer des Klassenzimmers ihres Kindes kennen und können damit auf die Aufnahmen aus diesem Raum zugreifen." Dadurch wird das System transparent und nachvollziehbar."

In die App soll auch eine Beschwerdefunktion integriert sein: „Wenn den Eltern etwas nicht gefällt und sie sich beschweren möchten, können sie dies

über die App tun." Das Problem werde dann von den Beamten in der entsprechenden Abteilung besprochen, erklärt das Bildungsministerium. Jederzeitigen Zugriff auf das Überwachungssystem sollen zudem autorisierte Beamte des Bildungsministeriums bekommen. So könnten sie Probleme in betroffenen Schulen erkennen und darauf reagieren.

Das Bildungsministerium hatte im September 2017 die Installation von Überwachungskameras in allen staatlichen Schulen angekündigt. Die Entscheidung folgte demnach auf die Vergewaltigung eines fünfjährigen Mädchens und dem Tod eines Jungen an zwei Schulen (Mewes, Indien: Videoüberwachung in Klassenzimmern für Eltern und Beamte, www.heise.de 18.01.2018).

China

Xinjiang erstellt unter falschem Vorwand Bevölkerungs-DNA-Datenbank

Von Juli bis Oktober 2017 wurden im Zuge von vermeintlichen Routineuntersuchungen DNA-Proben, Irisscans und Fingerabdrücke von Millionen ChinesInnen gesammelt. Offiziell war es ein Gesundheitscheck, angeboten von staatlichen Krankenhäusern, kostenlos für alle EinwohnerInnen der westchinesischen Provinz Xinjiang. Die Belege für diesen Datenmissbrauch finden sich ganz offen auf chinesischen Regierungswebsites. Die Menschenrechtsorganisation Human Rights Watch (HRW) hat sie zusammengetragen und am 13.12.2017 veröffentlicht. HRW-China-Direktorin Sophie Richardson: „Das Speichern der biometrischen Daten der Bevölkerung, einschließlich der DNA, ist eine grobe Verletzung internationaler Menschenrechtsnormen".

Insgesamt haben 18,8 Millionen EinwohnerInnen der Provinz an den Untersuchungen teilgenommen. Die Bevölkerung zwischen zwölf und 65 Jahren dürfte beinahe vollständig erfasst worden sein, und somit auch nahezu sämtliche Uiguren. Xinjiang ist die Heimat dieses muslimischen Turkvolks. Der Unmut unter den etwa neun Millionen Uiguren ist groß. Durch den Zuzug vieler Han-Chinesen stellen sie in Xinjiang nicht mehr die Mehrheit. Immer wieder kommt es zu Ausschreitungen. Die Regierung reagiert mit Härte.

Seit Ende August 2016 hat Xinjiang einen neuen Parteichef, Chen Quanguo, ein Law-and-Order-Mann, der zuvor in Tibet gedient hat. Unter Chens Führung hat sich die Lage in der Provinz noch einmal deutlich verschärft. Wer ins Ausland reisen möchte, muss nun einen Antrag stellen und nach der Rückkehr bei den Behörden Bericht erstatten. Im Februar 2017 kündigte die Regierung an, sämtliche Autos per GPS-Sender zu überwachen. An manchen Tankstellen bekommt man inzwischen nur noch Benzin, wenn man vorher sein Gesicht hat einlesen lassen. Bei Straßenkontrollen überprüft die Polizei immer häufiger das Smartphone, die Daten werden gespeichert und eine App wird installiert, die automatisch feststellt, ob man verbotene Videos angesehen hat.

In den ersten vier Monaten von Chens Amtszeit wurden etwa 30.000 neue Polizeistellen ausgeschrieben. Sein Vorgänger hatte in den acht Monaten zuvor 900 neue Sicherheitskräfte gesucht. 2017 sind mehr als 70.000 weitere Jobs geschaffen worden, hinzu kommen Zehntausende private Sicherheitsleute und Türsteher, die mit Schlagstöcken Restaurants und Läden bewachen müssen. Etliche Firmen für Sicherheitstechnik haben sich in den vergangenen drei Jahren in Xinjiang angesiedelt und Forschungs- und Entwicklungszentren eröffnet. Alles, was technisch machbar ist, wird inzwischen in Xinjiang an Menschen ausprobiert. Überwachungsdrohnen, Gesichtserkennung, Spyware – und jetzt auch DNA-Analysen (Giesen, Unter falschem Vorwand, SZ 14.12.2017, 7).

Technik-Nachrichten

Dating-Portale ohne Datenschutz

Die Stiftung Warentest hat den Datenschutz bei 44 Dating-Apps für Android und iOS untersucht und festgestellt, dass nur fünf Apps einen akzeptablen Schutz vorsehen. Damit Dating-Apps ein geeignetes Match zwischen zwei Personen anzeigen können, benötigen sie jede Menge private Daten von ihren Nutzenden: Wo sie wohnen, wie alt sie sind, ob sie Männer oder Frauen oder beides mögen. Obwohl deshalb guter Datenschutz wichtig wäre, kam die Stiftung Warentest zu ernüchternden Ergebnissen. Viele Anbieter senden Nutzer-Informationen an Werbefirmen oder Facebook. Mit den Daten der Dating-Apps können sie umfangreiche Nutzerprofile erstellen oder fehlende Daten ergänzen sowie personalisierte Werbung anzeigen. Nicht nur für die Werbewirtschaft, auch für Hacker können diese sehr persönlichen Daten interessant sein: 2015 konnten Angreifer Daten des Seitensprung-Portals Ashley Madison erbeuten und erpressten damit die Betreiber (DANA 3/2015, 148 f.).

Die Dating-Anbieter wissen sehr viel über ihre Nutzenden. Als die französische Journalistin Judith Duportail im September 2017 ihre Nutzungsdaten anforderte, erhielt sie 800 Seiten voller Details über ihr Liebesleben zurück. Sie konnte jede Nachricht nachlesen, die sie über die App verschickt hatte und beispielsweise nachschauen, wie alt die Männer waren, mit denen sie in Kontakt stand.

Schlecht geschützte Dating-Daten können gefährlich sein. So erhebt beispielsweise die App Grindr die Standortdaten des Nutzers. Die App soll homosexuelle Männer verbinden und wurde so in Staaten wie Ägypten mit schwulenfeindlichen Behörden zum Problem: Die Menschenrechtsorganisation Amnesty International berichtet, dass die Behörden in dem Land Grindr gezielt nutzen, um Homosexuelle ausfindig zu machen. Das deutsche Auswärtige Amt warnte vor diesem Vorgehen der ägyptischen Behörden.

Die Stiftung Warentest hat die kostenlosen Dating-Apps von 22 Anbietern untersucht, die jeweils für die mobilen Betriebssysteme Android und iOS verfügbar sind – also 44 Apps insgesamt. Darunter waren bekannte Anbieter wie Tinder, Elitepartner oder Parship. Untersucht wurde die Datenübertragung: Welche App sendet welche Daten an wen? Der Datenverkehr der untersuchten Apps wurde über einen speziellen Server geleitet und konnte so ausgelesen werden. Die Tester stuften Apps als kritisch ein, wenn sie Daten sendeten, die für den Betrieb des Dating-Services nicht notwendig sind, etwa die eindeutige Identifikationsnummer des Smartphones oder den Namen des Mobilfunkanbieters. Zusätzlich bewerteten sie Apps als kritisch, wenn die Profildaten der Nutzenden an Werbefirmen gesendet wurden, etwa ihr Alter. Zudem wurden die Datenschutzerklärungen der Anbieter untersucht. Ein Experte prüfte sie auf Genauigkeit und präzise Formulierungen, während ein Jurist nach Mängeln und Verstößen suchte.

Die Tester von Stiftung Warentest fanden fünf Apps (beziehungsweise App-Versionen) akzeptabel: Für Android waren das E-Darling, Lovescout 24 und Neu.de. In der Android- und der iOS-Version wurde nur die App Bildkontakte als akzeptabel eingestuft. Alle hielten ihre Datenschutzerklärungen auf Deutsch, juristische Mängel gab es nur sehr wenige. Allerdings sind die Testsieger bei den Informationen zur Nutzung in der Datenschutzerklärung auch nicht über ein „Ungenau" hinausgekommen. Den Datenverkehr der Dating-App Kiss No Frog haben die Tester zwar in beiden Versionen als unkritisch bewertet, allerdings war die Datenschutzerklärung sehr ungenau. Der Anbieter gab beispielsweise nicht an, welche Daten während eines Facebook-Logins verwendet werden.

Bei bekannten Anbietern stellte die Stiftung Warentest „erhebliche Schwächen" fest. So sendete Elitepartner Daten über den Mobilfunkanbieter und die Benutzungsstatistiken an Facebook. Darunter könnten Informationen fallen, welche Nutzenden wann oder wo die App verwendet haben. In der Datenschutzerklärung behält sich das Unternehmen zusätzlich das Recht vor, die IP-Adresse des Rechners für Werbung an Facebook zu senden. So könnten Werbeanbieter ihre Anzeigen personalisieren. Bei Parship dokumentierten die Tester dieselben Mängel. Auch die weit verbreitete App Tinder schickte den Namen des Mobilfunkanbieters an Facebook. Zudem sendete die iOS-Version der App Geräteinfos an eine US-Marketingfirma. In der Datenschutzerklärung schreibt das Unternehmen offen, dass es Nutzerdaten mit den Daten von Dritten kombiniert. Der komplette Test findet sich für ein Euro auf der Webseite von Stiftung Warentest sowie in der Zeitschrift „test 3/2018" (Strathmann, Ich weiß, wen du datest, SZ 22.12.2018, 24).

Rechtsprechung

BVerwG

BND muss Telefonie-Metadaten löschen

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat dem Bundesnachrichtendienst (BND) nach einem zweijährigen Rechtsstreit mit Urteil vom 13.12.2017 untersagt, Telefonie-Metadaten von Mitgliedern der Journalistenorganisation Reporter ohne Grenzen (ROG) sowie des Berliner Anwalts Niko Härting in seinem Verkehrsanalysesystem VerAS zu speichern und auszuwerten, weil dafür keine gesetzliche Grundlage besteht (Az. 6 A 6.16 u. 6 A 7.16).

Seit 2002 speichert der BND Telefonie-Metadaten in der Datei VerAS. Gesprächsinhalte sind von der Datenspeicherung nicht betroffen. Die Daten stammen aus der strategischen Fernmeldeüberwachung, der Ausland-Ausland-Fernmeldeaufklärung und dem Austausch mit anderen Nachrichtendiensten. In den Verhandlungen räumte der Geheimdienst ein, dass die dadurch abgebildeten Kontaktnetzwerke in beliebig weite Verzweigungen hinein analysiert werden können. Nach Auffassung von Reporter ohne Grenzen (ROG) können damit auch JournalistInnen erfasst werden, „die nur indirekt und über mehrere weitere Kommunikationspartner zum Beispiel mit einem Terrorverdächtigen in Verbindung gebracht werden können".

Soweit die Metadaten wie etwa Telefonnummern einzelnen Personen zugeordnet werden können, werden sie vom BND gemäß eigenen Angaben vor der Speicherung anonymisiert. Nach Einschätzung von ROG lassen sich die Daten aber dennoch oft individuell auswerten. Das BVerwG sieht in dem Vorgehen des BND einen Eingriff in das durch Art. 10 GG garantierte Fernmeldegeheimnis. Hierfür bedarf es einer gesetzlichen Grundlage. Das BVerwG urteilte, dass diese hier fehlt. Das G-10-Gesetz erlaubt nur die Speicherung zur Auswertung nach konkreten Suchbegriffen, nicht aber für eine Analyse der Verbindungen. Über den speziellen Fall hinaus wird wohl die Bewertung des Gerichts wirken, dass eine Anonymisierung der Metadaten nicht „der verfassungsrechtlich gebotenen Löschung gleichsteht". Mit dieser allgemeinen Aussage wird eine Vielzahl weiterer Sachverhalte in völlig anderen Zusammenhängen erfasst.

Reporter ohne Grenzen strebte mit seiner Klage ursprünglich an, nicht nur die Speicherung und Auswertung von Telefonie-, sondern auch Internet- und E-Mail-Metadaten zu untersagen. Das scheiterte jedoch daran, dass in der von der Klage erfassten Datei VerAS nur Telefonie-Daten verarbeitet werden. Die Journalistenorganisation erhob daher Anfang Dezember 2017 Beschwerde beim Europäischen Gerichtshof für Menschenrechte (EGMR), um die Auswertung aller Metadaten untersagen zu lassen. Christian Mihr, Geschäftsführer von ROG: „Durch das Urteil könnten nun auch andere Personen und Organisationen mit demselben Anliegen an den BND herantreten".

Wenige Tage zuvor hatten zur Kontrolle des BND berufene Juristen (ein Bun-

desanwalt und zwei RichterInnen beim Bundesgerichtshof) im vertraulichen Kreis der Geheimdienstkontrolleure im Bundestag, so der Vizevorsitzende des Bundestags-Kontrollgremiums André Hahn (Linke), „sehr schwerwiegende Vorwürfe" gegen den BND formuliert, weil durch den BND dem erst im Frühjahr 2017 nach einer BND-Gesetzesreform gebildeten Gremium „de facto die Arbeit unmöglich gemacht wird". Ähnlich äußerte sich der SPD-Obmann im Parlamentarischen Kontrollgremium Burkhard Lischka. Man werde die Vorwürfe gegen den BND genau prüfen. Sollte es „auch künftig" beim BND am Willen fehlen, sich juristischer Kontrolle auszusetzen, „müssen wir das Gesetz eben weiter verschärfen" (Schulzki-Haddouti, Bundesverwaltungsgericht: Bundesnachrichtendienst darf keine Telefonie-Metadaten nutzen, www.heise.de 14.12.2017; BND muss Daten löschen, SZ 15.12.2017, 5).

BGH

Arztbewertungsportal Jameda verletzte Neutralitätspflicht

Mit Urteil vom 20.02.2018 gab der Bundesgerichtshof (BGH) in Karlsruhe einer Dermatologin/Allergologin in Köln mit ihrer Klage gegen das Arztbewertungsportal Jameda Recht, wonach diese die Löschung ihres Profils fordern kann, wenn das Portal seine Neutralitätspflicht verletzt (Az. VI ZR 30/17). Unter der Internetadresse www.jameda.de betreibt die Beklagte, eine Tochter des Burda-Verlags, ein Arztsuche- und Arztbewertungsportal, auf dem Informationen über alle 275.000 niedergelassenen ÄrztInnen kostenfrei abgerufen werden können. Dies sind zunächst vom Portal bereitgestellte „Basisdaten" wozu akademischer Grad, Name, Fachrichtung, Praxisanschrift, weitere Kontaktdaten sowie Sprechzeiten und ähnliche praxisbezogene Informationen gehören. Daneben sind Bewertungen abrufbar, die Nutzende in Form eines Notenschemas, aber auch von Freitextkommentaren, abgegeben haben. Die Beklagte bietet den Ärzten den kostenpflichtigen Abschluss von Verträgen an, bei denen ihr Profil, anders als das Basisprofil der nichtzahlenden Ärzte, mit einem Foto und zusätzlichen Informationen versehen wird. Daneben werden beim Aufruf des Profils eines nichtzahlenden Arztes die Profilbilder unmittelbarer Konkurrenten gleicher Fachrichtung im örtlichen Umfeld mit Entfernungsangaben und Noten als „Anzeige" gekennzeichnet eingeblendet. Bei ÄrztInnen, die kostenpflichtig registriert sind und ein „Premium-Paket" gebucht haben, wurden keine Konkurrenten auf deren Profil angezeigt.

Die Klägerin wurde als Nichtzahlerin gegen ihren Willen mit ihrem akademischen Grad, ihrem Namen, ihrer Fachrichtung und ihrer Praxisanschrift geführt. Bei Abruf ihres Profils auf dem Portal der Beklagten erscheinen unter der Rubrik „Hautärzte (Dermatologen) (mit Bild) in der Umgebung" weitere (zahlende) ÄrztInnen mit demselben Fachbereich und mit einer Praxis in der Umgebung der Praxis der Klägerin. Dargestellt wurde neben der Note des jeweiligen anderen Arztes die jeweilige Distanz zwischen dessen Praxis und der Praxis der Klägerin. Die Klägerin erhielt in der Vergangenheit mehrfach Bewertungen. Sie beanstandete durch ihre früheren Prozessbevollmächtigten im Jahr 2015 insgesamt 17 abrufbare Jameda-Bewertungen, worauf nach deren Löschung ihre Gesamtnote von 4,7 auf 1,5 anstieg.

Die Klägerin verlangte von der Beklagten die vollständige Löschung ihres Eintrags in www.jameda.de, die Löschung ihrer auf der Internetseite www.jameda.de veröffentlichten Daten, die Unterlassung der Veröffentlichung eines sie betreffenden Profils auf der genannten Internetseite sowie Ersatz vorgerichtlicher Rechtsanwaltskosten. Das Landgericht Köln hatte die Klage mit Urteil vom 13.07.2016 abgewiesen (28 O 7/16). Die Berufung der Klägerin beim Oberlandesgericht Köln blieb am 05.01.2017 ohne Erfolg (15 U 121/16).

Auf die Revision hiergegen wurde der Klägerin Recht gegeben. Nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Zwar hatte der BGH mit Urteil vom 23.09.2014 (VI ZR 358/13) in Bezug auf Jameda im Grundsatz entschieden, dass eine Speicherung der personenbezogenen Daten mit einer Bewertung der ÄrztInnen durch PatientInnen zulässig ist. Anders als dort ging es aber hier um die Frage der Stellung als „neutraler" Informationsmittler. Während das Portal bei den nichtzahlenden ÄrztInnen dem ein Profil aufsuchenden Internetnutzenden die „Basisdaten" nebst Bewertung des betreffenden Arztes anzeigt und ihm mittels des eingeblendeten Querbalkens „Anzeige" Informationen zu örtlich konkurrierenden Ärzten bietet, lässt sie auf dem Profil der „Premium"-KundInnen – ohne dies den Internetnutzenden hinreichend offenzulegen – solche über die örtliche Konkurrenz unterrichtenden werbenden Hinweise nicht zu. Der BGH forderte, dass sich Jameda in dieser Weise zugunsten ihres Werbeangebots in ihrer Rolle als „neutraler" Informationsmittler zurücknehmen müsse. Dann könne sie mit ihrer auf das Grundrecht der Meinungs- und Medienfreiheit (Art. 5 Abs. 1 Satz 1 GG, Art. 10 EMRK) gestützten Rechtsposition gegenüber dem Recht der Klägerin auf Schutz ihrer personenbezogenen Daten (Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK) ein höheres Gewicht erlangen. Anders im konkreten Fall, wo die Grundrechtsposition der Klägerin überwog und ihr ein „schutzwürdiges Interesse an dem Ausschluss der Speicherung" ihrer Daten (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG) zugebilligt wurde.

Bei Jameda werden täglich im Schnitt etwa 1.500 Bewertungen erstellt. Diese durchlaufen zunächst einen automatischen Prüfalgorithmus, bei dem kontrolliert wird, ob mehrere Bewertungen für eine ÄrztIn von der gleichen IP-Adresse stammen, oder ob es Indizien dafür gibt, dass eine ÄrztIn sich selbst eine Bewertung erstellt. Gemäß Unternehmensangaben werden ca. 10% der Bewertungen sofort gelöscht. Weitere auffällige Bewertungen würden von insgesamt 20 Mitarbeitenden im Rahmen einer Qualitätssicherung genauer geprüft. Extreme Bewertungen ergäben sich, so Jameda, wenn PatientInnen nach einer Behandlung „emotionalisiert" seien.

Zu massenhaften Löschungen von Ärzteprofilen wird es nach dem BGH-Urteil nicht kommen, da Jameda – offenbar

vorbereitet auf die juristische Niederlage – umgehend reagierte und die vom BGH beanstandeten Anzeigen konkurrierender ÄrztInnen abgeschaltet hat. Geschäftsführer Florian Weiß erklärte, damit bestehe kein Löschungsanspruch; Jameda werde auch weiterhin vollständige Ärztelisten zeigen. Tatsächlich hatte der Senatsvorsitzende Gregor Galke bei der Urteilsverkündung erklärt, an der grundsätzlichen Zulassung von Jameda festzuhalten, da solche Geschäftsmodelle – ihre Neutralität vorausgesetzt – ihren „legitimen Platz" im Feld der Meinungsfreiheit hätten. Damit blieb das Gericht im Grundsatz bei der Linie, die seit seinem ersten Urteil zu den Zensuren für Lehrkräfte auf spickmich.de besteht. Stets hatte die Meinungsfreiheit den Vorrang vor den Datenschutzinteressen der Betroffenen. So wurde die Bewertung von Hotels, von ÄrztInnen oder – beim Europäischen Gerichtshof für Menschenrechte – von AnwältInnen für zulässig erachtet. Der inhaltliche Spielraum, den die Gerichte den Bewertungen gewähren, ist groß; es wurden schon Attribute wie „Hühnerhof" (für ein Hotel) oder „Psychopath" (für einen Hochschulprofessor) gebilligt.

In jüngster Zeit scheint die Haltung zu Bewertungsportalen generell skeptischer geworden zu sein. 2016 verpflichtete der BGH Jameda zu Nachforschungen, falls ein Betroffener die Bewertung für unbegründet hielt. Auch außerhalb der Gerichte lassen sich kritische Bestandsaufnahmen beobachten. Im Herbst 2017 kündigte das Bundeskartellamt an, sich die Portale hinsichtlich ihrer Transparenz und wirtschaftlichen Verflechtungen genauer anzusehen. Das Bundesjustizministerium befasst sich mit dem Thema Bewertungsportale. Der Präsident der Bundesärztekammer Frank Ulrich Montgomery forderte ein Gesetz, wonach die ÄrztInnen selbst entscheiden können sollen, ob sie gelistet werden oder nicht. Es wird über die gesetzliche Regulierung von Vergleichs- und Bewertungsportalen diskutiert, und dabei über Transparenz, Neutralität und Abwehransprüche. Als problematisch werden weiterhin die Premium-Konten gesehen, da die Berufsordnungen der Ärztekammern strenge Regeln für das Marketing vorsehen, so z. B. die in Bayern: „Berufswidrig ist insbesondere eine nach Inhalt und Form anpreisende, irreführende oder vergleichende Werbung". Kritik kommt auch von den Verbraucherzentralen. Diese favorisieren als nicht gewinnorientiertes Bewertungsportal die „Weisse Liste". Dieses von der Bertelsmann-Stiftung finanzierte Portal steht unter der Schirmherrschaft der Patientenbeauftragten des Bundes (BGH, Bundesgerichtshof zur Speicherung und Übermittlung personenbezogener Daten im Rahmen eines Arztsuche, PE 20.02.2018; Janisch, Noten für Ärzte – Richter ziehen Grenzen/ Unehrliche Makler, SZ 21.02.2018, S. 14; von der Hagen/Hütten, Jameda macht einfach weiter, SZ 22.02.2018, 20).

BGH

Keine Prüfpflicht von Google vor Aufnahme in Suchindex

Der Bundesgerichtshof (BGH) urteilte am 27.02.2018, dass Google als Betreiber einer Internet-Suchmaschine nicht verpflichtet ist, sich vor der Anzeige eines Suchergebnisses darüber zu vergewissern, ob die von den Suchprogrammen aufgefundenen Inhalte Persönlichkeitsrechtsverletzungen beinhalten (Az. VI ZR 489/16). Der Suchmaschinenbetreiber muss erst reagieren, wenn er durch einen konkreten Hinweis von einer offensichtlichen und auf den ersten Blick klar erkennbaren Verletzung des allgemeinen Persönlichkeitsrechts Kenntnis erlangt.

Die Kläger, ein Ehepaar, das als IT-Dienstleister tätig ist und in einem Internet-Forum u. a. als „Schwerstkriminelle", „Terroristen", „Bande" und „krimineller Stalkerhaushalt" bezeichnet worden war, forderten von Google die Unterlassung, diese persönlichkeitsrechtsverletzenden Inhalte über die Suchmaschine auffindbar zu machen. Die Suchmaschine wirft für ihre Nutzenden entsprechend dem eingegebenen Suchbegriff nach einem eigenen Algorithmus eine Ergebnisliste aus und verlinkt diese.

Die Kläger hatten ab Mitte Februar 2011 beim Aufsetzen eines F-Internetforums geholfen. Mitglieder dieses Forums führten mittels Beiträgen auf verschiedenen Forenseiten Auseinandersetzungen mit Mitgliedern eines anderen G-Internetforums. Den Mitgliedern des F-Internetforums wurde u. a. vorgeworfen, Dritte zu stalken und zu drangsalieren. Aufgrund einer von dem Kläger im Rahmen seiner Tätigkeit für das F-Internetforum eingerichteten E-Mail-Weiterleitung stellten Dritte die IP-Adresse und die Identität des Klägers fest und gaben diese Informationen an Mitglieder des mit dem F-Internetforum verfeindeten G-Internetforums weiter. Letztere verfassten sodann auf den mit der Klage beanstandeten Internetseiten Beiträge, in denen der Kläger für Handlungen von Mitgliedern des F-Internetforums (unter anderem angebliches Stalking) verantwortlich gemacht wurde. Die auf der Google-Ergebnisliste nachgewiesenen Seiten enthielten deshalb Inhalte, wonach der Kläger das F-Internetforum betreibe, für die dort veröffentlichten Inhalte (mit-)verantwortlich sei oder von den Inhalten des Forums zumindest Kenntnis gehabt habe und die Klägerin von der Rolle ihres Mannes in diesem Forum Kenntnis gehabt haben müsse.

Das Landgericht Köln hatte der Unterlassungsklage in der ersten Instanz teilweise stattgegeben. Das Berufungsgericht hat die Klage insgesamt abgewiesen. Die Revision gegen diese Abweisung hatte keinen Erfolg. Der BGH meinte, dass den Klägern gegen Google keine Ansprüche wegen Verletzung des allgemeinen Persönlichkeitsrechts zustehen. Die beanstandeten Inhalte seien keine eigenen Inhalte der Beklagten. Sie wurden von anderen Personen ins Internet eingestellt. Google mache sich die Inhalte durch Aufnahme in den Suchindex nicht zu Eigen. Das Unternehmen durchsucht lediglich mit Hilfe von Programmen die im Internet vorhandenen Seiten und erstellt hieraus automatisiert einen Suchindex. Zwar könne Google grundsätzlich auch als sog. mittelbare Störerin haften, wenn sie zu der Verletzung des allgemeinen Persönlichkeitsrechts willentlich und mitursächlich beiträgt, indem sie im Internet Beiträge auffindbar macht. Eine Haftung des Suchmaschinenbetreibers setze aber eine Verletzung von Prüfpflichten voraus. Vernünftigerweise könne nicht erwartet werden, dass Google sich ver-

gewissert, ob die von den Suchprogrammen aufgefundenen Inhalte rechtmäßig ins Internet eingestellt worden sind, bevor diese auffindbar gemacht werden. Die Annahme einer – praktisch kaum zu bewerkstelligenden – allgemeinen Kontrollpflicht würde die Existenz von Suchmaschinen als Geschäftsmodell, das von der Rechtsordnung gebilligt worden und gesellschaftlich erwünscht sei, ernstlich in Frage stellen. Ohne die Hilfestellung einer solchen Suchmaschine wäre das Internet aufgrund der nicht mehr übersehbaren Flut von Daten für den Einzelnen nicht sinnvoll nutzbar. Den Betreiber einer Suchmaschine treffen gemäß dem Urteil erst dann spezifische Verhaltenspflichten, wenn er durch einen konkreten Hinweis Kenntnis von einer offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung erlangt hat.

Davon ging der BGH im Streitfall nicht aus. Die beanstandeten Bezeichnungen der Kläger waren zwar ausfallend scharf und beeinträchtigten ihre Ehre. Ihr ehrbeeinträchtigender Gehalt stand aber nicht von vornherein außerhalb jedes in einer Sachauseinandersetzung wurzelnden Verwendungskontextes, da die Äußerungen ersichtlich im Zusammenhang mit der Rolle der Kläger beim F-Internetforum standen. Nach dem Inhalt der beanstandeten Suchergebnisse werden den Mitgliedern des F-Internetforums u. a. Stalking (Straftat gemäß § 238 StGB) vorgeworfen. Der Kläger hatte eingeräumt, am „Aufsetzen" des F-Internetforums beteiligt gewesen zu sein und durch eingerichtete E-Mail-Weiterleitung auch später daran aktiv beteiligt gewesen zu sein. Über eine eigene, durch „eidesstattliche Versicherung" bekräftigte, aber ziemlich allgemein gehaltene und pauschale Behauptung hinaus, mit dem F-Internetforum nichts zu tun zu haben, hatte der Kläger keine belastbaren Indizien für die Haltlosigkeit der ihm – und zumindest mittelbar in Form der Mitwisserschaft seiner Frau, der Klägerin, – gemachten Vorwürfe aufgezeigt. Eine offensichtliche und auf den ersten Blick klar erkennbare Rechtsverletzung musste Google den beanstandeten Äußerungen deshalb nicht entnehmen. Der BGH knüpft damit an eine Entscheidung aus dem Jahr 2017 an, wonach Google grds. nicht haftet, wenn in einer Bildersuche illegal ins Internet eingestellte Fotos erscheinen (BGH, Bundesgerichtshof zur Prüfungspflicht des Betreibers einer Internet-Suchmaschine (www.google.de) bei Persönlichkeitsrechtsverletzungen, PM Nr. 39/18 v. 27.02.2018; Fuchs, Nachher reicht, SZ 28.02.2018, 27).

BGH

EuGH-Vorlageverfahren wegen Datenschutzeinwilligung

Mit Beschluss vom 05.10.2017 legte der Bundesgerichtshof (BGH) dem Europäischen Gerichtshof (EuGH) Fragen zur Cookie-Richtlinie, also dem Art. 5 Abs. 3 Telekommunikations-Datenschutzrichtlinie (TK-DSRl) und zur Datenschutzeinwilligung vor (Az. I ZR 7/16). Der BGH möchte wissen, ob es im Sinne der europäischen Datenschutzrichtlinie (EG-DSRl) sowie der neuen, ab 25.05.2018 anwendbaren Datenschutzgrundverordnung (DS-GVO) bei der Anwendung des Art. 5 Abs. 3 TK-DSRl für die dort geforderte Einwilligung ausreicht, dass ein voreingestelltes Ankreuzkästchen nicht abgewählt wurde. Außerdem will der BGH wissen, ob es insofern einen Unterschied macht, ob durch das Cookie-setzen personenbezogene oder nicht-personenbezogene Daten erhoben werden sollen. Gefragt wird schließlich, welche Informationen vor Erteilung einer Einwilligung bereitgestellt werden müssen, insbesondere zur Funktionsdauer der Cookies und in Bezug auf die Stellen, die auf die Cookies Zugriff nehmen können.

Kläger in dem Verfahren ist der Verbraucherzentrale Bundesverband (vzbv), der im Rahmen eines Verbandsklageverfahren sich gegen einen Gewinnspielbetreiber im Internet zur Wehr setzt, der für E-Mail-, SMS-, Telefon- und Postbewerbung eine aktive Einwilligung der Teilnehmenden erbittet, für das Setzen von Cookies aber ein vorangekreuztes Zustimmungsfeld aufführt, bei dem zwecks Zustimmungsverweigerung der Haken entfernt werden muss. Der vzbv meint, die verwendeten Einwilligungen und die dazu erteilten Informationen seien ungenügend und deshalb nicht wirksam. Mit dieser Meinung drang er zwar beim erstinstanzlichen Landgericht weitgehend durch, in geringerem Maße aber beim Berufungsgericht. Dieses vertrat die Meinung, dass die Möglichkeit des Entfernens des vorausgefüllten Häkchens genüge und die Stellen, die auf die Cookies zugreifen können, nicht genannt werden müssten. Gegen dieses Urteil legten beide Seiten beim BGH Revision ein.

Dem EuGH-Vorlageverfahren geht ein jahrelanger juristischer Streit voraus, nachdem 2009 die TK-DSRl geändert worden war: Zuvor genügte es für das Setzen von Cookies, dass den Betroffenen eine Widerspruchsmöglichkeit eingeräumt wird; danach wird gemäß Art. 5 Abs. 3 eine Einwilligung für das Setzen von Werbecookies gefordert. Während in anderen EU-Mitgliedstaaten nach 2009 das Recht angepasst wurde und dabei teilweise eine explizite Einwilligung, teilweise aber nur das Ermöglichen eines Widerspruchs (Opt-out) gefordert wird, blieb der deutsche Gesetzgeber inaktiv. Von Anfang an gilt § 15 Abs. 3 Telemediengesetz (TMG), der für den Fall der Erstellung pseudonymer Profile für Werbe- und Marketingzwecke eine Widerspruchsmöglichkeit für ausreichend erklärt. Seitdem kritisieren die deutschen Verbraucher- und Datenschützer, dass die Cookie-Regelung der EU nicht umgesetzt sei und das TMG insofern gegen Europarecht verstößt.

Die Rechtslage wird dadurch verkompliziert, dass die TK-DRSl in Bezug auf die Voraussetzungen für die Einwilligung auf die EG-DSRl verweist, die bisher durch § 4a BDSG-alt umgesetzt wurde. Die EG-DSRl und das BDSG-alt werden aber nur bis zum 24.05.2018 anwendbar sein; danach gilt für Einwilligungen die DSGVO. Art. 94 Abs. 2 DSGVO sieht vor, dass Verweisungen in anderem Recht auf die EG-DSRl künftig durch die entsprechenden Regelungen der DSGVO ersetzt werden. D. h. ab dem 25.05.2018 gilt gemäß den klaren Verweisungsregelungen die gegenüber dem § 4a BDSG verschärfte und technisch angepasste Regelung des Art. 7 DSGVO. Der BGH hatte bisher geurteilt, dass das Belassen eines vorangekreuzten Fel-

des als Einwilligung angesehen werden kann. Diese Ansicht lässt sich, das sieht der BGH anscheinend selbst so, mit der Wirksamkeit der DSGVO nicht mehr halten.

Sowohl das alte Datenschutzrecht (EG-DSRl und BDSG-alt) wie auch die DSGVO sind aber grundsätzlich nur auf Verarbeitung von Daten natürlicher Personen anwendbar. Anders aber die TK-DSRl, die auch für juristische Personen gilt. Der Verweis in der TK-DSRl auf die EG-DSRl und damit auch auf die neue DSGVO macht keine Unterscheidung zwischen personenbezogenen und sonstigen Daten. Die Frage des BGH, ob die Einwilligungsanforderungen auch gelten, wenn kein Personenbezug besteht, hat wohl in diesem unterschiedlichen Anwendungsbereich ihren Grund.

Spannend ist auch die Frage nach den vor Abgabe der Einwilligung erforderlichen Informationen. Webseitenbetreiber waren insofern oft sehr nachlässig. Es ist aus Datenschutzsicht ein gewaltiger Unterschied, ob Cookies werbepartnerübergreifende Profile ermöglichen sollen oder nicht.

Die Cookie-Regelung der TK-DSRl wird absehbar durch eine zeit- und technikgemäßere Regelung in der geplanten ePrivacy-Verordnung ersetzt werden. Die ursprüngliche Hoffnung, dass diese ePrivacy-Verordnung zeitgleich mit der DSGVO zur Anwendung gebracht werden kann, erwies sich als Illusion. Es wird noch einige Zeit dauern, bis die ePrivacy-Verordnung ausdiskutiert, beschlossen und in Kraft ist. Daher ergibt sich die ungute Situation, dass das Telekommunikationsdatenschutzrecht alt ist, der allgemeine Datenschutz in der DSGVO aber auf der Höhe der Zeit. Der EuGH hat mit der BGH-Vorlage die Möglichkeit, nicht nur bestehende, sondern auch dadurch neu entstehenden Unwuchten zu reparieren.

BGH

Ex-Präsidentenbilder vom Supermarkt sind zulässig

Der Bundesgerichtshof (BGH) entschied auf eine Klage des ehemaligen Bundespräsidenten Christian Wulff gegen einen Zeitschriftenverlag mit Urteil vom 06.02.2018, dass dieser Bilder des Klägers bei einem Supermarkt-Besuch veröffentlichen darf (Az. VI ZR 76/17). Am 06.05.2015 hatte Wulff in einer Pressemitteilung bestätigt, dass er und seine Frau wieder zusammen lebten. Am 13.05.2015 veröffentlichte die Zeitschrift „People“ unter der Überschrift „Liebes-Comeback“ einen Artikel über den Kläger und seine Ehefrau und bebilderte diesen Artikel u. a. mit einem Foto, das den Kläger und seine Ehefrau am Auto zeigte. Am 20.05.2015 veröffentlichte der beklagte Verlag in der Zeitschrift „Neue Post“ unter der Überschrift „Nach der Versöhnung - Christian Wulff - Wer Bettina liebt, der schiebt!“ einen weiteren Artikel über den Kläger und seine Ehefrau und bebilderte den Artikel u. a. mit einem Foto des Klägers mit einem gefüllten Einkaufswagen. Das Landgericht hat der auf Unterlassung der Bildberichterstattung gerichteten Klage stattgegeben. Die Berufung der Beklagten hatte keinen Erfolg. Nach Ansicht des Oberlandesgerichts verletzte die Veröffentlichung der Bilder den Kläger in seiner Privatsphäre.

Der VI. Zivilsenat des BGH hob die Vorentscheidungen auf und wies die Klage Wulffs ab mit der Begründung, dass die veröffentlichten Fotos dem Bereich der Zeitgeschichte (§ 23 Abs. 1 Nr. 1 KunstUrhG) zuzuordnen seien und deshalb auch ohne Einwilligung des Klägers (§ 22 KunstUrhG) verbreitet werden durften. Berechtigte Interessen des Abgebildeten würden damit nicht verletzt. Nach Ansicht des BGH hatten die Vorinstanzen die in besonderer Weise herausgehobene Stellung des Klägers als ehemaliges Staatsoberhaupt, den Kontext der beanstandeten Bildberichterstattung sowie das Ausmaß der vom Kläger in der Vergangenheit praktizierten Selbstöffnung nicht hinreichend berücksichtigt und deshalb rechtsfehlerhaft dem Persönlichkeitsrecht des Klägers den Vorrang vor der durch Art. 5 Abs. 1 GG geschützten Pressefreiheit der Beklagten eingeräumt.

Die herausgehobene politische Bedeutung des Klägers als Inhaber des höchsten Staatsamtes und das berechtigte öffentliche Interesse an seiner Person endeten nicht mit seinem Rücktritt vom Amt des Bundespräsidenten; die besondere Bedeutung des Amtes wirke vielmehr nach. Auch nach seinem Rücktritt erfülle der Kläger, der als „Altbundespräsident“ weiterhin zahlreichen politischen und gesellschaftlichen Verpflichtungen nachkommt, Leitbild- und Kontrastfunktion auch in der Normalität seines Alltagslebens. Im Zusammenhang mit der – nicht angegriffenen – Textberichterstattung leisteten die Veröffentlichungen einen Beitrag zu einer Diskussion allgemeinen Interesses. Sie nähmen Bezug auf die vom Kläger selbst erst einige Tage zuvor durch Pressemitteilung bestätigte Versöhnung mit seiner Frau. Gegenstand der Berichterstattung sei darüber hinaus die eheliche Rollenverteilung. Die Fotos bebilderten dies und dienten zugleich als Beleg. In der Neuen Post wurde über die „Rollenverteilung in der Partnerschaft zwischen Mann und Frau“ berichtet, dass Wulff Mineralwasser, Salat und Schokoküsse eingekauft habe, also Dinge, die ihm sicherlich Bettina aufgeschrieben habe. Der Kläger habe selbst sein Ehe- und Familienleben in der Vergangenheit immer wieder öffentlich thematisiert und sich dadurch mit einer öffentlichen Erörterung dieses Themas einverstanden gezeigt. Die zur Einkaufszeit auf dem Parkplatz eines Supermarktes und damit im öffentlichen Raum aufgenommenen Fotos beträfen den Kläger lediglich in seiner Sozialsphäre. Senatsvorsitzender Gregor Galke wies darauf hin, dass der Parkplatz eines Supermarktes gleichsam öffentlich sei, auch bei privaten Verrichtungen. Den entgegenstehenden berechtigten Interessen des Klägers käme demgegenüber kein überwiegendes Gewicht zu (§ 23 Abs. 2 KunstUrhG). Die Fotos wiesen keinen eigenständigen Verletzungsgehalt auf, sondern zeigten den Kläger in einer unverfänglichen Alltagssituation und in der Rolle eines fürsorgenden Familienvaters. In einem BGH-Urteil zu Fotos von Sabine Christiansen hatte das Gericht 2009 noch ausgeführt: „Private Lebensvorgänge sind auch dann Teil der geschützten Privatsphäre, wenn sie im öffentlichen Raum stattfinden“ BGH, PE v. 06.02.2018, Bundesgerichtshof gestattet die Veröffentlichung von Bildern des ehemaligen Bundespräsidenten Christian Wulff bei einem Supermarkteinkauf; Janisch, Öffentlicher Einkauf, SZ 07.02.2018, 27).

OVG NRW

Fahrerbewertung.de unzulässig

Das Oberverwaltungsgericht (OVG) Nordrhein-Westfalen (NRW) in Münster hat mit Urteil vom 19.10.2017 festgestellt, dass das Portal „Fahrerbewertung.de“, wie von der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW festgestellt, datenschutzrechtlich unzulässig ist (Az. 16 A 770/17). Dort kann, wer meint, einen Drängler oder Raser entdeckt zu haben, unter Eingabe des Autokennzeichens dessen Fahrverhalten mit den Farben Rot, Gelb oder Grün bewerten - im benannten Fall vermutlich mit Rot.

Dieser hübsche Zeitvertreib für die mobile Gesellschaft versprach den Betreibern bisher viel Traffic und Werbeeinnahmen. Diese beteuerten ihre hehren Absichten: Man wolle die Fahrer mittels schlechter Noten zur „Selbstreflexion“ anhalten und dadurch zur Sicherheit im Straßenverkehr beitragen. Wer sich dafür interessiert, ob der freundliche Nachbar oder Kollege auch auf der Autobahn ein netter Mensch ist, könne mal schnell dessen Kfz-Kennzeichen eintippen.

Die LDI NRW machte dem Portal Auflagen, insbesondere untersagte sie den allgemeinen Zugang zu den individuellen Bewertungen. Es brauche keine „Nebenjustiz“ in Form einer privaten Verkehrssünderkartei. Vor Gericht ging es zunächst darum, ob Kfz-Kennzeichen personenbezogene Daten sind. Das wäre fraglich, wenn der Normalautofahrer ohnehin kaum an den Namen hinter der Nummer gelangen könnte. Aus Sicht des Verwaltungsgerichts Köln als erste Instanz, das den Datenschützern ebenso Recht gegeben hatte, ist das Nummernregister ein erstaunlich offenes Buch: Man müsse dem Kraftfahrt-Bundesamt (KBA) nur ein „rechtlich relevantes Interesse“ (also eine Schramme im Blech) vorspiegeln, und schon bekomme man den gewünschten Namen.

Das OVG NRW bestätigte, dass das Portal tief in das Recht auf Datenschutz eingreift, weil „eine vollständig anonyme Bewertung von in der Regel privat motiviertem Verhalten für eine unbegrenzte Öffentlichkeit einsehbar“ sei. Die Richter hielten also missbräuchliche Bewertungen für wahrscheinlich. Und für die Betroffenen könnten die Fahrnoten negative Konsequenzen haben: Arbeitgeber oder Versicherungen könnten sich für die Bewertungen interessieren. Fraglich sei zudem, ob der Datenpranger die wahren Übeltäter wirklich dazu veranlasst, den Fuß vom Gaspedal zu nehmen. Dazu müssten sie ja davon erfahren, was der Betreiber nicht sicherstellt. Nach der Verfügung der LDI können Fahrer-Bewertungen durchaus zulässig sein, wenn der Fahrzeughalter der Einzige ist, der von seinen Noten Kenntnis erhält. Gemäß dem Gericht würde dies genügen, um ihn zur „Selbstreflexion“ anzuhalten. Die Nichtzulassungsbeschwerde gegen das OVG-Urteil wurde vom Bundesverwaltungsgericht zurückgewiesen. Die LDI will sich nun darum kümmern, dass wieder rechtskonforme Verhältnisse hergestellt werden (Janisch, Richter rügen Online-Pranger für Autofahrer, www.sueddeutsche.de 23.10.2017).

OLG Frankfurt/Main

Datenschutzverstoß hindert vertragliche Ersatzansprüche

Das Oberlandesgericht Frankfurt am Main (OLG) hat mit Urteil vom 24.01.2018 entschieden, dass ein Adresskäufer wegen Unwirksamkeit des Kaufvertrags keine vertraglichen Ansprüche in Bezug auf eine anstößige Datennutzung durch Dritte hat, wenn wirksame Einwilligungen der Adressinhaber nach dem Bundesdatenschutzgesetz (BDSG) fehlen; auch ein bereicherungsrechtlicher Anspruch nach § 816 Abs. 1 BGB wird ausgeschlossen (Az.: 13 U 165/16).

Die mit Adressdaten handelnde Klägerin nahm den beklagten Insolvenzverwalter der vormals ebenfalls mit Adressdaten handelnden Schuldnerin in Anspruch. Der Geschäftsführer der Klägerin war zuvor Geschäftsführer der Schuldnerin. Er hatte am Tag der Insolvenzeröffnung von der Beklagten verschiedene Internet-Domains einschließlich darüber generierte Adressen für 15.000 € gekauft. Die Daten befanden sich ursprünglich auf zwei Servern der Schuldnerin und wurden auf einem USB-Stick übergeben. Die Server selbst, auf denen die Daten weiterhin rekonstruierbar lagen, wurden vom Beklagten an eine ebenfalls mit Adressen handelnde dritte Firma verkauft. Diese nutzte gemäß dem Klägervortrag rund eine Million Adressen, um Werbe-E-Mails für die Internetseite „sexpage.de“ zu versenden.

Die Klägerin klagte deshalb aus abgetretenem Recht ihres Geschäftsführers auf Schadenersatz und Unterlassen. Sie vertrat die Ansicht, die von ihr erworbenen Adressen hätten durch die erfolgte Nutzung für die Internetseite „sexpage.de“ 2/3 ihres Wertes verloren. Der Beklagte müsse deshalb den Kaufpreis anteilig an sie zurückzahlen. Zudem sei er verpflichtet, die weitere Nutzung dieser Adressdaten zu unterlassen. Das Landgericht gab der Klage statt. Dagegen legte die Beklagte Berufung ein.

Die Berufung beim OLG hatte Erfolg. Das OLG urteilte, dass der Klägerin keinerlei vertragliche Ansprüche zustehen. Der Kaufvertrag sei vielmehr insgesamt nichtig, da die Adressinhaber in den Verkauf ihrer Daten nicht wirksam eingewilligt hätten. Der Vertrag verstoße gegen die Vorgaben des BDSG. Die Nutzung personenbezogener Daten sei nur zulässig, wenn der Betroffene einwillige oder das sogenannte Listenprivileg eingreife. Name, Postanschrift, Telefonnummer und E-Mail-Adresse einer Person stellten klassische personenbezogene Daten dar. Der auch nur einmalige Verkauf derartiger Daten unterfalle dem Adresshandel im Sinne des § 28 Abs. 3 S. 1 BDSG. Das sogenannte Listenprivileg nach § 28 Abs. 3 S. 2 BDSG sei nicht anwendbar, da es sich nicht um „zusammengefasste Daten von Angehörigen einer bestimmten Personengruppe“ handele.

Laut OLG ist eine Einwilligung nach dem BDSG nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, der auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hingewiesen werde. Sie müsse grundsätzlich schriftlich abgegeben werden. Außerdem sei sie besonders hervorzuheben, wenn sie – wie hier – zusammen mit anderen Erklä-

rungen erteilt werde. Nach dem von der Klägerin selbst vorgetragenen Wortlaut der Einwilligungserklärung seien jedoch weder die betroffenen Daten noch Kategorien etwaiger Datenempfänger oder der Nutzungszweck – Adresshandel – konkret genug bezeichnet worden. Es fehlte zudem die erforderliche Hervorhebung.

Weiter führt das OLG aus, dass der Vertrag die Parteien systematisch zu einem unlauteren wettbewerbswidrigen Verhalten verpflichte, sodass auch deshalb von einer Gesamtnichtigkeit auszugehen sei. Die Zusendung von Werbe-E-Mails ohne Einwilligung stelle eine unzumutbare Belästigung nach § 7 Abs. 2 Nr. 3 UWG dar.

Das OLG verneint auch einen bereicherungsrechtlichen Rückzahlungsanspruch der Klägerin. Zwar sei der Beklagte im Ergebnis in Höhe des erlangten Kaufpreises ungerechtfertigt bereichert. Ein bereicherungsrechtlicher Rückzahlungsanspruch sei hier aber ausgeschlossen, da beide Vertragsparteien vorsätzlich gegen die zwingenden Vorgaben des BDSG verstoßen hätten. Bei gesetzeswidrigen Verträgen versage § 817 Abs. 1 BGB jede Rückabwicklung. Wer sich dennoch auf ein derartiges Geschäft einlasse, leiste auf eigenes Risiko (rsw.beck-online.de, OLG Frankfurt am Main: Adresskäufer hat bei fehlender Einwilligung der Adressinhaber keinerlei Ansprüche wegen anstößiger Datennutzung durch Dritte, 29.01.2018).

VG Dresden

Auskunftsanspruch erstreckt sich auf Schriftwechsel

Mit Urteil vom 26.07.2017 wurde der Mitteldeutsche Rundfunk, für den der Beitragsservice der Rundfunkanstalten tätig ist, vom Verwaltungsgericht (VG) Dresden dazu verurteilt, einem Beitragspflichtigen Auskunft nicht nur über die dort gespeicherten Stammdaten, sondern auch über den mit diesem geführten und gespeicherten Schriftwechsel zu geben (Az. 6 K 1372/15).

Der Beitragsservice hatte sich im Rahmen eines Meldedatenabgleichs die Adressdaten des Klägers besorgt und ihn hierüber und über seine Beitragspflicht informiert. Daraufhin beantragte der Kläger zweimal eine Datenschutzauskunft beim Beitragsservice. Als er auch nach 6 Monaten noch keine Antwort erhalten hatte, klagte er vor dem VG. Daraufhin informierte der Beitragsservice den Kläger über gespeicherte Namen, Geburtsangaben, Adressen und Kontodaten und meinte, damit seine datenschutzrechtliche Pflicht erfüllt zu haben. Der Kläger verlangte, darüber hinaus auch Kopien des gespeicherten Schriftverkehrs zu erhalten. Zur Verhandlung erschien kein Beklagtenvertreter.

Das VG ließ die Klage als Verpflichtungsklage zu, weil die Entscheidung über ein Auskunftsbegehren ein Verwaltungsakt sei. Bei der Auskunftserteilung gemäß dem Sächsischen Datenschutzgesetz (SächsDSG) handele es sich nicht nur um die Vornahme eines Realaktes. Ein Vorverfahren durch Einlegen eines Widerspruchs sei hier nicht erforderlich gewesen, weil der Beitragsservice „nicht in angemessener Frist entschieden" habe. In der Sache vertrat das VG die Ansicht, dass die bisher erteilte Auskunft den rechtlichen Anforderungen nicht entspricht, da dem Kläger „ein Verzeichnis über die beim Beklagten gespeicherten Schriftsätze" nicht übersandt wurde: „Es gilt der Grundsatz der bestmöglichen Auskunft". „Auch der Schriftverkehr zwischen Kläger und Beitragsservice bzw. Beklagtem beinhaltet personenbezogene Daten des Klägers, soweit der Kläger darin versucht, die Voraussetzungen des Härtefalls mit Angaben zu seinen persönlichen Verhältnissen zu begründen. Die genannten Daten wurden ausweislich der vorliegenden Verwaltungsakte auch vom Beitragsservice gespeichert." Das Gericht benannte die Defizite der erteilten unvollständigen Auskunft: „Aus ihr ist weder der zweite Vornamen noch der Familienstand der Klägers ersichtlich. Auch ist für den Kläger aus dieser Auskunft nicht ersichtlich, welche Schriftstücke aus der zwischen ihm und dem Beitragsservice geführten Korrespondenz Verwaltungsakte geworden sind. Dem Beklagten hätte es damit zumindest oblegen, dem Kläger ein sog. Verfahrensverzeichnis zur Kenntnis zu geben, aus dem der Kläger ersehen kann, welche Daten der Beklagte zu ihm gespeichert hat und welche Daten zur Person grundsätzlich beim Beklagten gespeichert werden.

Entgegen der Auffassung des Klägers gewährt § 18 Abs. 1 Nr. 1 SächsDSG jedoch keinen Anspruch auf Übersendung von Aktenauszugskopien. Denn § 18 Abs. 1 SächsDSG verpflichtet die datenverarbeitende Stelle ausschließlich zur Erteilung von Auskünften. Entscheidend ist demnach die Vermittlung des Informationsgehaltes der gespeicherten Daten in der deutschen Sprache. Weder kann hiernach die Herausgabe von Aktenbestandteilen noch die Anfertigung und Übersendung von Kopien der selbigen verlangt werden. In welcher Form der Beklagte dem begründeten Begehren des Klägers auf Auskunftserteilung nachkommt, hat er nach pflichtgemäßem Ermessen in eigener Verantwortung zu entscheiden."

LG Berlin

Facebook unterliegt bei Voreinstellungen und Einwilligungen

Das Landgericht (LG) Berlin hat mit Urteil vom 16.01.2018 nach einer Klage des Verbraucherzentrale Bundesverbands (vzbv) entschieden, dass Facebook mit seinen Voreinstellungen und Teilen der Nutzungs- und Datenschutzbedingungen gegen geltendes Verbraucherrecht verstößt (Az. 16 O 341/15). Die Einwilligungen zur Datennutzung, die sich das Unternehmen einholt, sind nach dem Urteil teilweise unwirksam. Nach dem Bundesdatenschutzgesetz (BDSG) dürfen personenbezogene Daten nur mit Zustimmung der Betroffenen erhoben und verwendet werden. Damit diese bewusst entscheiden können, müssen Anbieter klar und verständlich über Art, Umfang und Zweck der Datennutzung informieren. Das Urteil ist nicht rechtskräftig. Sowohl der vzbv wie auch Facebook wollen Berufung einlegen.

Facebook genügt gemäß dem Urteil nicht den rechtlichen Anforderungen. So war in der Facebook-App für Mobiltelefone bereits ein Ortungsdienst aktiviert, der Chat-PartnerInnen den

eigenen Aufenthaltsort verrät. In den Einstellungen zur Privatsphäre war per Häkchen voreingestellt, dass Suchmaschinen einen Link zur Chronik der TeilnehmerIn erhalten. Dadurch wird das persönliche Facebook-Profil für jedeN schnell und leicht auffindbar. Die Richter entschieden, dass alle fünf vom vzbv monierten Voreinstellungen auf Facebook unwirksam sind. Es sei nicht gewährleistet, dass diese von Nutzenden überhaupt zur Kenntnis genommen werden.

Das LG erklärte außerdem acht Klauseln in den Nutzungsbedingungen für unwirksam. Diese enthielten unter anderem vorformulierte Einwilligungserklärungen, wonach Facebook Namen und Profilbild der Nutzenden „für kommerzielle, gesponserte oder verwandte Inhalte“ einsetzen und deren Daten in die USA weiterleiten durfte. Die Richter stellten klar, dass mit solchen vorformulierten Erklärungen keine wirksamen Zustimmungen zur Datennutzung erteilt werden können. Unzulässig ist auch eine Klausel, mit der sich Nutzende verpflichten, auf Facebook nur ihre echten Namen und Daten zu verwenden. Heiko Dünkel, Rechtsreferent beim vzbv: „Anbieter von Online-Diensten müssen Nutzern auch eine anonyme Teilnahme, etwa unter Verwendung eines Pseudonyms, ermöglichen. Das schreibt das Telemediengesetz vor.“ Nach Auffassung des Gerichts konnte dieser Aspekt aber offen bleiben, denn die Klausel sei bereits deshalb unzulässig, weil Nutzer damit versteckt der Verwendung dieser Daten zustimmten.

Nicht durchsetzen konnte sich der vzbv gegen die Werbung, Facebook sei kostenlos. Der Werbespruch ist nach Ansicht des Verbands irreführend. Dünkel erläutert: „Verbraucher bezahlen die Facebook-Nutzung zwar nicht in Euro, aber mit ihren Daten. Und diese bringen dem Unternehmen viel Geld ein.“ Dem gegenüber hielt das LG Berlin diese Werbung für zulässig, immaterielle Gegenleistungen seien nicht als Kosten anzusehen. Die Richter lehnten außerdem mehrere Anträge des vzbv gegen Bestimmungen in der Facebook-Datenrichtlinie ab. Die Richtlinie enthalte fast nur Hinweise und Informationen zur Verfahrensweise des Unternehmens und keine vertraglichen Regelungen (vzbv, Facebook verstößt gegen deutsches Datenschutzrecht, www.vzbv.de 12.02.2018).

LG Saarbrücken

Schweiger darf öffentliche Kritikerin namentlich nennen

In einem Verfahren einer Facebook-Nutzerin und dem Schauspieler Til Schweiger um einen Facebook-Eintrag des Schauspielers entschied das Landgericht (LG) Saarbrücken am 23.11.2017, dass dieser seinen die Frau betreffenden Post nicht löschen muss. Der Filmstar habe zwar das Persönlichkeitsrecht der Klägerin verletzt, als er eine private Nachricht der Saarländerin mit ihrem Namen und Foto auf seiner Facebook-Seite veröffentlichte. Der Vorsitzende Richter Martin Jung erklärte, dies sei aber vom Informationsinteresse der Öffentlichkeit und dem Recht Schweigers auf Meinungsfreiheit gedeckt. Die Klägerin, so das Gericht, habe ja „aus eigenem Antrieb“ an einer kontroversen öffentlichen Debatte teilgenommen. Und sich dabei nicht neutral geäußert, sondern Schweiger „in nicht unerheblicher Weise“ angegriffen. Sie hatte den Schauspieler nach der Bundestagswahl gefragt, ob er nun Deutschland verlassen werde, wie er es vor der Wahl im Fall eines Einzugs der AfD in den Bundestag angekündigt habe. Schweiger bestritt, diese Aussage gemacht zu haben. Zudem hatte die Klägerin Schweiger massiv kritisiert: „Ihr Demokratieverständnis und Ihr Wortschatz widern mich an.“ Der 53jährige Schauspieler antwortete ihr darauf; „hey schnuffi…! Date!? Nur wir beide!?“ und stellte einen Screenshot des Chats auf seine Seite. Danach hagelte es Kommentare, in denen die Saarländerin auch beschimpft und verspottet wurde.

Das LG urteilte, dieser Kritik müsse sie sich stellen. Ihre Aufforderung an Schweiger, das Land zu verlassen, sei „von kaum zu unterschätzender Bedeutung“. Die Frau leidet nach eigener Aussage seit dem Post erheblich unter den Kommentaren, auch gesundheitlich. Sie habe sogar eine Morddrohung erhalten. Deshalb wollte sie vor Gericht eine Löschung des Posts von Schweiger erzwingen. Sie sei weder Mitglied noch Sympathisantin der AfD. Das Gericht entschied, dass der Schauspieler die Frau auch namentlich nennen dürfe, da die Saarländerin den Schlagabtausch mit Schweiger selbst in einem Internetforum mit 25.000 Mitgliedern öffentlich gemacht habe, bevor sie vor Gericht auf Unterlassung klagte. Im Forum „Deutschland mon amour“ hatte sie kurz nach der Veröffentlichung angeblich Rat suchen wollen. Da sie dabei auch ihren vollen Namen und Wohnort nannte, sei dies „eine bewusste Selbstöffnung“ gewesen. Somit könne sie sich nicht mehr auf den Schutz der Privatsphäre berufen. Ihr Verhalten zeige, dass sie in der politischen Auseinandersetzung „gerade nicht völlige Anonymität und Zurückgezogenheit sucht“. Die Klägerin muss auch die Kosten des Verfahrens tragen.

Schweiger war weder bei der mündlichen Verhandlung noch bei der Verkündung des Urteils anwesend, obwohl das LG für die Verhandlung das persönliche Erscheinen beider Parteien angeordnet hatte. Ein Gerichtssprecher hatte vor Beginn der Verhandlung betont, dass die Kammer Wert darauf lege, dass beide Seiten persönlich erscheinen: „Das ist üblich in Fällen von Verletzungen des Persönlichkeitsrechts.“ Schweiger brauchte für sein Fehlen eine „besondere Entschuldigung“. Die betrachtete das Gericht allerdings durch die Vertretung seiner Anwälte als gegeben. Im Prozess hatte die Frau angegeben, Schweiger „provozieren und erzieherisch auf ihn einwirken“ zu wollen. Sie habe ihm mitteilen wollen, dass es nicht ihrem Demokratieverständnis entspreche, wenn man den politischen Gegner beschimpfe. Schweiger hatte über seine Anwältin erklären lassen, er habe mit dem Öffentlichmachen des Posts „gegen Hetze gleich welcher Art“ vorgehen und auf das Problem von Hass-Nachrichten aufmerksam machen wollen. Die Frau sei von der Gerichtsentscheidung enttäuscht, erklärte ihr Anwalt Arnold Heim (Facebook-Streit Til Schweiger bekommt Recht: Klägerin muss sich Kritik stellen, www.shz.de/18400426 23.11.2017; Til Schweiger gewinnt Prozess um Facebook-Eintrag, www.sueddeutsche.de 23.11.2017; Til Schweiger gewinnt Streit um Facebook-

Post gegen Kritikerin, www.heise.de 23.11.2017).

AG München

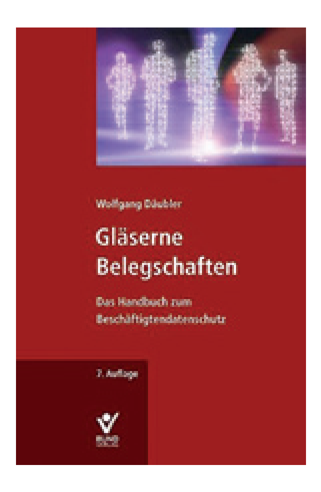
Kein Anspruch auf Entsperrung eines gefundenen Handys

Ein Richter des Amtsgerichts (AG) München hat mit Urteil vom 24.07.2017 rechtskräftig entschieden, dass der Finder eines verlorenen Smartphones keinen Anspruch gegenüber dem Hersteller hat, dass dieser eine dort vorgenommene Sperrung freischaltet, auch wenn der Finder an dieser Sache das Eigentum erworben hat (Az. 213 C 7386/17).

Anlass der Entscheidung war, dass ein Finder 2016 in einem Straßengraben ein iPhone fand, das er im Fundbüro abgab. Da der ehemalige Besitzer sich auch nach sechs Monaten nicht gemeldet hatte, erwarb der Finder gemäß § 973 Bürgerliches Gesetzbuch (BGB) rechtmäßig Eigentum an dem Smartphone. Der neue Eigentümer wollte anschließend das mit einem Sperrcode geschützte iPhone vom Apple Support freischalten lassen. Die Mitarbeitenden von Apple verweigerten jedoch die Freischaltung des Handys ohne Angabe einer Begründung. Daraufhin erhob der Finder als neuer Eigentümer des Handys Klage beim AG München gegen Apple, jedoch ohne Erfolg. Der Mann hat keinen Anspruch auf Entsperrung des Fundes.

Zwar sei der Mann durch den Fund und den Zeitablauf Eigentümer des Handys geworden. Jedoch erwerbe man als Finder das Eigentum lediglich in dem Zustand, in dem es sich nach Ablauf der sechs Monate nach dem Fund befindet. Der Finder habe also Eigentum an einem gesperrten und damit für ihn nicht nutzbaren iPhone erworben. Ein freigeschaltetes iPhone sei zu keinem Zeitpunkt Fundgegenstand gewesen. Ein Anspruch auf Freischaltung wurde vom AG München auch wegen erheblicher datenschutzrechtlicher Bedenken abgelehnt. Die Freischaltung würde den Zugriff auf sämtliche auf dem Telefon befindlichen Daten des ursprünglichen Inhabers ermöglichen, was mit dem Sperren des Mobiltelefons gerade verhindert werden soll. Insbesondere gelte dies angesichts der Tatsache, dass im vorliegenden Fall nicht geklärt sei, wo und unter welchen Umständen der ursprünglichen Eigentümer das Gerät verloren habe (Solmecke, AG München, Apple muss gefundenes iPhone nicht entsperren, 26.09.2017; Kant, Datenschutz: Apple muss gefundenes iPhone nicht entsperren, www.netzwelt.de 29.09.2017).

Buchbesprechungen



Däubler, Wolfgang,
Gläserne Belegschaften
7. Aufl. 2017, Bund-Verlag Frankfurt, ISBN 978-3-7663-6620-7, 678 S.

Es handelt sich um einen Klassiker: Wer eine betroffenenfreundliche Interpretation des Datenschutzrechts in Beschäftigungsverhältnissen schnell und informativ nachlesen möchte, der kommt am „Däubler" kaum vorbei (siehe zur Vorauflage DANA 1/2015, 54 f.). Während noch in der vorhergehenden 6. Auflage hinter „gläsernen Belegschaften" ein Fragezeichen gesetzt war, verzichtet die Neuauflage hierauf. Dies mag der technologischen Entwicklung und der Praxis geschuldet sein, die Beschäftigte für den Arbeitgeber immer „gläserner" machen. Und so widmet sich das Buch auch detailliert all den technischen Anwendungsfällen, mit denen Beschäftigte überwacht werden (können), von der Telekommunikationskontrolle über Videoüberwachung und Erfassung von Gesundheitsdaten bis hin zu Big-Data-Auswertungen, sowohl aus der individualrechtlichen wie auch aus der kollektivrechtlichen Sicht.

Das Buch ist auf dem neuesten Stand und berücksichtigt nicht nur umfassend die Datenschutz-Grundverordnung, sondern auch schon das neue Bundesdatenschutzgesetz und dessen Sonderregelung in § 26. Es unterscheidet sich von den vielen sonstigen systematischen Darstellungen, die es inzwischen auch zum Arbeitnehmerdatenschutz gibt, dadurch, dass viele anschauliche Beispiele aus der Praxis in einer unjuristischen Sprache, aber durchgängig arbeitnehmerfreundlich und rechtlich korrekt dargestellt werden. Dadurch bekommt das Handbuch großen Nutzen für die betriebliche Praxis insbesondere der Betriebsräte. Durch eine feingranulare Gliederung nach Randnummern

und mit vielen Zwischenüberschriften, die strukturell aus den Vorauflagen übernommen wurden, und durch ein detailliertes Inhalts- und Stichwortverzeichnis wird man schnell auch bei einer spezifischen Suche fündig. Man wird dann auch nicht mit der Meinung des Autors allein gelassen, sondern auf die wichtigste weitergehende Literatur und Rechtsprechung verwiesen. Ein äußerst umfangreiches Literaturverzeichnis erleichtert das Auffinden spezieller Veröffentlichungen.



Roßnagel, Alexander (Hrsg.)
Das neue Datenschutzrecht
Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze
Nomos 2018, 477 Seiten, ISBN 978-3-8487-4411-4, 58,00 €

(tw) Nach Schantz/Wolff (DANA 4/2017, 180 f.) ist das von Alexander Roßnagel herausgegebene Sammelwerk die zweite umfassende systematische Darstellung des neuen Datenschutzrechtes unter Einschluss des – ebenso wie die Datenschutz-Grundverordnung (DSGVO) – vom 25.05.2018 an anzuwendenden Bundesdatenschutzgesetzes (BDSG). Sie geht auf die wissenschaftliche Untersuchung der Europäischen Datenschutz-Grundverordnung (2017) zurück, ist aber erheblich detaillierter und tiefer gehend und hat diesmal nicht die nationale Umsetzung der DSGVO, sondern deren Anwendung im Blick, ohne sich dabei rechtspolitische Aussagen zu verkneifen. Dabei wird weitgehend die aktuelle Literatur einbezogen und auf eine Vielzahl von unklaren Rechtsfragen eingegangen. Gleich geblieben ist die stark wissenschaftliche Herangehensweise, bei der dann praktische Fragen oft weniger im Fokus stehen.

Das Buch ist, wie bei Roßnagel schon hinlänglich bekannt, von einer äußerst DSGVO-kritischen Sicht geprägt. Der Herausgeber behauptet, mit der DSGVO werde das Datenschutzniveau in Deutschland gesenkt. Dabei redet er die gewaltigen Chancen klein, die sich mit der DSGVO ergeben. Gegenüber der bisherigen Rechtslage eröffnen sich – gerade wegen der von Roßnagel kritisierten Technikneutralität und Unbestimmtheit und Entwicklungsbedürftig- wie -fähigkeit – Perspektiven, die mit der alten Rechtslage absolut verbaut geblieben wären. Angesichts der Offenheit vieler Abwägungsfragen bestehen – was Roßnagel zugesteht – weitgehende Konkretisierungsmöglichkeiten wie auch -notwendigkeiten.

Es handelt sich um ein wissenschaftliches Sammelwerk, bei dem die einzelnen Kapitel von den AutorInnen individuell verantwortet werden. Angesichts deren Vielzahl (22) verfolgt das Gesamtwerk keine inhaltlich völlig kohärente Linie. Anders aber als in anderen Sammelwerken, wo eine Linie oft überhaupt nicht erkennbar ist und verarbeitungs- und grundrechtsfreundliche Positionen unvermittelt nebeneinanderstehen, ist hier eine grundrechts- bzw. betroffenenfreundliche Handschrift des Herausgebers eindeutig erkennbar. Dessen ungeachtet finden sich Aussagen, die bei einer kritischen Hinterfragung kaum Bestand haben können, etwa, wenn Jandt die Ansicht vertritt, § 29 Abs. 2 BDSG mit seiner Einschränkung der Kontrollkompetenz der Datenschutzaufsicht sei europarechtskonform.

Auch wenn manchen Positionen in dem Werk nicht zugestimmt werden sollte, so liefert es die bisher wohl umfassendste systematische Analyse der ab 25.05.2018 geltenden Rechtslage und spricht eine Vielzahl von bisher nur verstreut oder noch nicht angesprochenen Fragen an, die hier – unter Angabe von weiterführenden Quellen – zwischen zwei Einbandsdeckeln zu finden sind. Ein ausführliches Normenverzeichnis erleichtert das Auffinden einschlägiger Aussagen, während das Stichwortverzeichnis oft wenig weiter hilft, um auf spezifische Fragen Antworten zu finden. Erfreulich umfangreich ist auch das Literaturverzeichnis, wenngleich insofern wegen des dauernd hinzukommenden Materials noch lange keine Konsolidierung eintreten wird. Das gilt auch für vielen aufgeworfenen Fragen, zu denen Hinweise, aber längst noch keine allgemeingültigen Antworten gegeben werden.

Cartoon



Endlich eine „Sicherheit“, die den Geschmack des neuen Innenministers trifft



Das überarbeitete bayerische Polizeiaufgabengesetz...

◆ erlaubt der Polizei Wohnungen heimlich abzuhören und zu filmen ◆ erlaubt Gesichtserkennung auf Demonstrationen ◆ erlaubt Zugriff auf Smartphones, Computer und die Cloud ◆ erlaubt Kommunikationsverbindungen durch den Einsatz technischer Mittel zu unterbrechen oder zu verhindern ◆ erlaubt in informationstechnischen Systemen auch Daten zu löschen oder zu verändern ◆ erlaubt künftig präventiv Post zu beschlagnahmen, bei Gefahr im Verzug auch ohne richterliches Einverständnis ◆ erleichtert die Übermittlung personenbezogener Daten durch die Polizei an „nichtöffentliche Stellen“, zum Beispiel an Geheimdienste, im Inland und Ausland ◆ erlaubt geheimdienstliche Befugnisse für die Polizei ◆ erlaubt die erweiterte DNA-Analyse ◆ erlaubt, Bürger präventiv als Gefährder zu kategorisieren ◆ erlaubt Aufenthaltsverbote und -gebote für so genannte Gefährder ohne richterlichen Vorbehalt ◆ erlaubt „unendliche Haft“ ◆ erlaubt den Einsatz von Handgranaten

https://www.bayern.landtag.de/www/ElanTextAblage_WP17/Drucksachen/Basisdrucksachen/0000013000/0000013038.pdf

Bild: ClipDealer